IP Surveillance Handbook

Network Cameras | Video Servers | Video Receiver | Network Video Recorder | Central Management Software

VIVOTEK
BUILT WITH RELIABILITY

Welcome to
Planet VIVOTEK

About VIVOTEK:

VIVOTEK Inc., founded in 2000, has quickly taken its place as a leading manufacturer in the IP surveillance industry. VIVOTEK specializes in the integration of audio-visual components into network operation. Using sophisticated codec technologies, VIVOTEK's innovative R&D team develops a wide range of multimedia communication products. In 2006, VIVOTEK became a publicly traded company in the Taiwan Stock Exchange offering sales, support, and other services in over 70 countries through a wide network of distributors and system integrators.

Table of Contents

Chap.1 IP Surveillance Overview 01

1.1 Overview 01
1.2 Network Cameras 01
1.2.1 Introduction 01
1.2.2 Camera Types 03
1.3 Video Servers 04
1.4 Network Video Recorders 05
1.5 Central Management Software 05
1.6 Evolution of Video Surveillance 06

Chap.2 Lens and Image Sensor Technology 07

2.1 Lens 07
2.1.1 Focal Length 07
2.1.2 Iris 08
2.1.3 Lens Mount Types 09
2.2 Image Sensor 11
2.2.1 Sensor Types 11
2.2.2 Resolutions 11
2.2.3 Sensor Scan Modes 13
2.2.4 Wide Dynamic Range 14
2.3 Lens and Image Sensor Considerations 14
2.3.1 Lens Form Factors for Image Sensor 14
2.3.2 View Angle 15
2.3.3 Day and Night 15

Chap.3 Video and Audio Compression 19

3.1 Video Compression 19
3.1.1 MJPEG 19
3.1.2 MPEG-4 20
3.1.3 H.264 21
3.2 Audio Compression 22
3.2.1 G.711 22
3.2.2 AMR 22
3.3.3 AAC 22
3.3 Video and Audio Streaming 23
3.3.1 Multiple Streams 23
3.3.2 Two-way Audio 23

Table of Contents

Chap.4 IP Network 25

4.1 Network Types 25
4.2 Network Devices 25
4.3 IP Address 26
4.4 Network Protocols 27
4.4.1 Device Connection 27
4.4.2 Transmission Protocols 30
4.4.3 Video Transmission Methods 30
4.4.4 Event Notification 31
4.4.5 Timing Correction 31
4.4.6 Video Quality Control 31
4.5 Wireless Networks 32
4.5.1 WiFi 32
4.5.2 3GPP 32
4.5.3 WiMAX 32
4.6 Security 33
4.6.1 IP Filtering 33
4.6.2 Username and Password 33
4.6.3 Security Protocols 33
4.6.4 Security Wireless Transmission 34
4.7 PoE 35

Chap.5 Camera Housing and Mounting 37

5.1 Housing 37
5.1.1 Vandal-proof 37
5.1.2 Weather-proof 37
5.1.3 Covering 38
5.2 Mounting 39
5.3 Scanner 40

Chap.6 Bandwidth and Storage 41

6.1 Bandwidth Management 41
6.1.1 Assessing Demands 41
6.1.2 Calculation 41
6.2 Storage 41
6.2.1 Assessing Demands 41
6.2.2 Storage Media 42
6.3 Redundancy 43
6.3.1 Cables 43
6.3.2 RAID 43

Table of Contents

Chap.7 Video Management 45

7.1 Video Management Platforms 45
7.1.1 PC-based 45
7.1.2 NVR-based 46
7.2 Basic Features of Software 47
7.2.1 Monitoring 47
7.2.2 Recording 48
7.2.3 Playback 48
7.2.4 Management 49
7.3 Advanced Features 49
7.3.1 E-map 49
7.3.2 Auto-backup 49
7.3.3 Failure Report 49
7.4 Digital I/O Devices 49
7.4.1 Digitial Input Devices 49
7.4.2 Digital Output Devices 50
7.5 Managing Large Systems 50

Chap.8 Applications 51

Chap.9 System Design 53

9.1 Identifying Customer Needs 53
9.1.1 Viewing Considerations 53
9.1.2 Environmental Considerations 54
9.2 System Planning 58
9.2.1 Camera Considerations 58
9.2.2 Hardware Considerations 58
9.2.3 Software Considerations 58
9.3 Installation and Checks 58
9.3.1 On-site Installation 58
9.3.2 Post-installation Checks 58
9.4 Operational Training 59
9.5 System Maintenance 60

Chap.10 Intelligent Video Systems 61

10.1 Introduction 61
10.2 Architecture 61
10.2.1 Centralized Platform 61
10.2.2 Distributed Platform 62
10.3 Advantages of Distributed Architecture 63
10.4 Detection 63
10.4.1 Tamper Detection 63
10.4.2 Intelligent Motion Detection 64
10.4.3 Loitering Detection 65
10.4.4 License Plate Recognition 65
10.4.5 People Counting 66

Glossary 67

Chap.1
IP Surveillance Overview

1.1 Overview

Increasing penetration of the Internet and the development of innovative technologies have encouraged rapid growth of the IP surveillance industry, driving changes in the video surveillance market. It is expected that IP surveillance will be dominating the video surveillance market in the near future, with network cameras and video servers being major trends.

An IP surveillance digitizes video streams and transmits them over networks, allowing users to view and manage the video and images remotely with a networked device, such as a PC, anytime and anywhere. Key components of an IP surveillance system consist of network cameras, video servers, network video recorders and central management software. VIVOTEK provides a full range of products mentioned above to help customers build a reliable and high performance IP surveillance system that meets their needs.

IP surveillance products are being used in a variety of application fields, which generally fall into the following four categories:

- **Professional applications:** transportation, government, industrial, construction, health care, etc.
- **SMB applications:** banking, education, retailing, recreation, etc.
- **Home applications:** residential surveillance, digital home, etc.
- **3GPP applications:** mobile surveillance, elder care, baby or pet viewing, etc.

1.2 Network Cameras

1.2.1 Introduction

A network camera, also known as Internet camera, IP camera or Internet video camera, transmits live digital video over an Ethernet network to back-end devices such as a PC or 3G phone. With a dedicated IP address, a built-in web server and audio/video streaming protocols, it can work independently for real-time monitoring.

Images from network cameras can be viewed with a web browser such as Internet Explore, Firefox, Mozilla and Opera, enabling customers to perform live viewing on different networked devices. In addition, customers can control and manage multiple cameras at the same time in any places where network connection is available. Therefore, an IP surveillance system is easier and more convenient to use compared with a CCTV system.

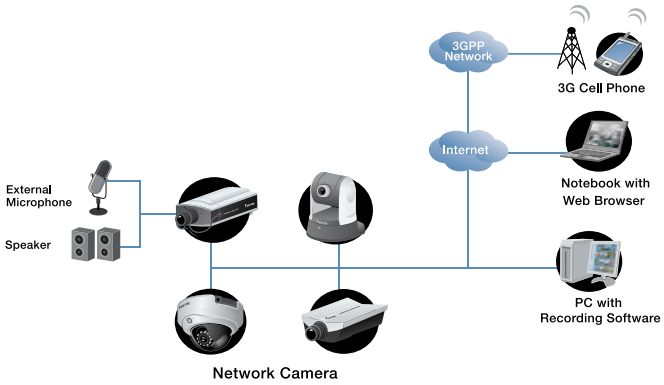


Figure 1.1 Network camera connection

A network camera mainly consists of a lens, an image sensor, an image processor, a video compression SoC (System on Chip) and an Ethernet chip that offers network connectivity for data transmission (Figure 1.2).

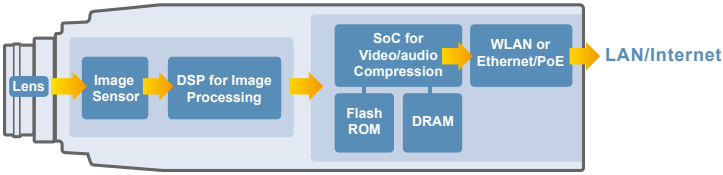


Figure 1.2 Network camera composition

When light passes through the lens to the sensor, it is converted to digital signals and then processed by a built-in digital signal processor. The processed video data is then compressed by a multimedia SoC to achieve a smaller data size for optimal transmission. Finally, the video images are sent through the Internet to back-end devices to allow for viewing and storage. Apart from video compression, the SoC is built with a RISC CPU for processing system and network data.

The general interface of a network camera includes a power cord socket, an Ethernet socket, audio I/O ports and digital I/O ports (Figure 1.3).

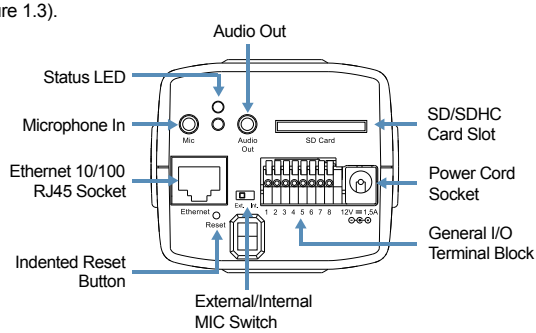


Figure 1.3 General interface of network camera

In addition to a full-range IP surveillance product lineup, VIVOTEK has achieved competitive advantages over other rivals in terms of multimedia SoC design, EE & ME integration and multimedia SDK. With these capabilities, VIVOTEK is able to provide highly integrated products with superior image quality, comprehensive customer services and versatile application solutions.

1.2.2 Camera Types

Generally, network cameras can be divided into four types for different applications, including fixed, pan/tilt/zoom, fixed dome and speed dome.

Fixed Type

A fixed network camera points in a fixed direction to monitor a specific area, such as hallways, staircases or corridors. Because people can be aware of the camera's shooting direction, in some cases, it can deter vandalism and crimes.

A fixed network camera usually comes with a RS-232/422/485 interface that connects the cameras to a pan/tilt scanner for wider coverage.

Many fixed network cameras has exchangeable C/CS-mount lens design, giving users the ability to change the lens to adapt for different monitoring conditions. For more information on C/CS-mount, please refer to Chapter 2.

Figure 1.4 Fixed network camera

Pan/Tilt/Zoom Type

Capable of changing shooting direction horizontally and vertically to achieve a wide field of view, a pan/tilt network camera is used in many spacious areas, such as lobbies or parking lots.

Some pan/tilt network cameras are integrated with zoom capability so as to provide close-up images of distant objects. Users can easily control PTZ functions through a web browser.

Figure 1.5 PTZ network camera

Fixed Dome Type

A fixed dome network camera, mostly designed for indoor surveillance, has a housing to make the object of interest less aware of where the camera is pointing at. With a 3-axis mechanism, images can remain in an upright orientation when it is installed either against the wall or on the ceiling. Furthermore, the design of a fixed dome network camera can better fit in with the decor.

A fixed dome network camera can be furnished with a weather- or vandal-proof housing for outdoor applications.

Figure 1.6 Fixed dome network camera

Speed Dome Type

Compared with fixed dome type, a speed dome network camera is integrated with pan, tilt and zoom capabilities, enabling a far greater field of view. With a high zoom capability, image stabilization and 360-degree endless pan, a speed dome camera is mainly used for professional applications, such as airports, banks or city security.

Figure 1.7 Speed dome network camera

1.3 Video Servers

A video server is a device that converts analog signals to digital, allowing users to migrate to a digital surveillance system without replacing existing CCTV systems.

A video server mainly includes a compression chip and an Ethernet chip, with two main types available: one port or four ports.

Figure 1.8 Video server

1.4 Network Video Recorders

An NVR (Network Video Recorder) is an IP-based recorder that operates independently from a PC or other operation systems. Aimed to store digital video streams from network cameras, an NVR is usually incorporated with a large-volume hard disk to allow for a long period of recording.

An NVR differs from a traditional DVR in its network connectivity, which allows digital data to be transmitted to other networked devices over the Internet. Another difference is that an NVR can be directly connected to a network camera while a DVR is usually be connected to an analog camera.

VIVOTEK's NR7401 helps you build a high-efficiency surveillance system, where you can simultaneously record, monitor and manage video data through the Internet. NR7401 works seamlessly with all VIVOTEK network cameras.

Figure 1.9 Network video recorder

1.5 Central Management Software

Central management software, often provided by the camera vendors or individual software vendors, enables customers to manage and control cameras from remote site. Typically, central management software is windows-based, and thus can be installed in almost any PC.

Central management software employs client-server architecture where server software,client viewing software and playback software is installed in separate PCs. Customers can perform live viewing, event-triggered recording or playback on the client PC while managing cameras and performing constant recording with the server PC. Each server PC can be scaled up to include several subordinate server PCs, and thus expand the number of managed cameras.

VIVOTEK ST7501 central management software works seamlessly with VIVOTEK's full-range network cameras and video servers, helping customers establish a robust, flexible and efficient platform for centralized video management.

Figure 1.10 Central management software

1.6 Evolution of Video Surveillance

For two decades of evolution, video surveillance has progressed from fully analog to fully digital. The development of surveillance systems is segmented into three periods, known as the first, second and third generation.

The first-generation surveillance system consists of the use of analog CCTV cameras, multiplexers, analog monitors and VCRs. Camera images are transmitted via coaxial cables and stored in VCR cassettes. Due to limited storage capacity, the cassettes must be replaced frequently for a long period of recording.

The early 1990s saw the emergence of the second-generation surveillance system, which is composed of CCTV cameras, DVRs and digital monitors. Analog camera images are digitized and stored in DVRs. The replacement of VCRs by DVRs gives users more flexibility in data viewing and storage. Around 2005, demand for network-enabled DVR picked up, and pure network-enabled NVRs were introduced. NVRs provide remote data access and management capability.

The third-generation surveillance system, also known as IP surveillance, appeared in early 2000. The surveillance system uses network cameras and takes full advantage of the TCP/IP Internet. Users can remotely control, monitor and record live video (Figure 1.11).

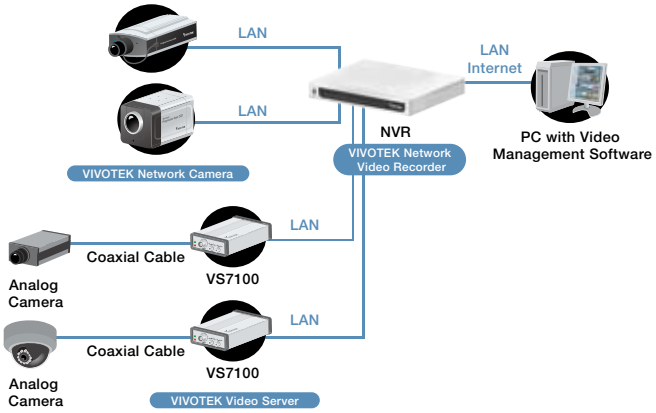


Figure 1.11 IP surveillance system architecture

Advantages of IP Surveillance

- **Remote monitoring/storage**

Since video data can be transmitted to remote networked devices over Ethernet networks, users can view camera images in any place where IP network connection is available.

- **Cost efficiency**

Video surveillance systems can leverage existing IP network infrastructure, significantly reducing overall installation costs.

- **High scalability**

Adding new network cameras or other networked devices in an IP surveillance system is easy by simply connecting them to a router.

- **Superior image quality**

Network cameras provide high image quality; many of them even offer megapixel resolutions. In addition, IP surveillance has no signal degradation problems during transmission, and thus can ensure steady image quality.

Chap.2
Lens and Image Sensor Technology

2.1 Lens

The generation of a high quality image is decided by many factors including light source of the environment, lens, sensor, compression engine, etc. However, for camera itself, a lens is the most fundamental component that firstly decides if the output of the quality is good or not. In the security industry, because the use of camera differs, especially fixed type with C/CS mount, system installers themselves have to select and purchase a lens fitting their specific needs.

2.1.1 Focal Length

Focal length is the distance between the sensor and secondary principal point of the lens.

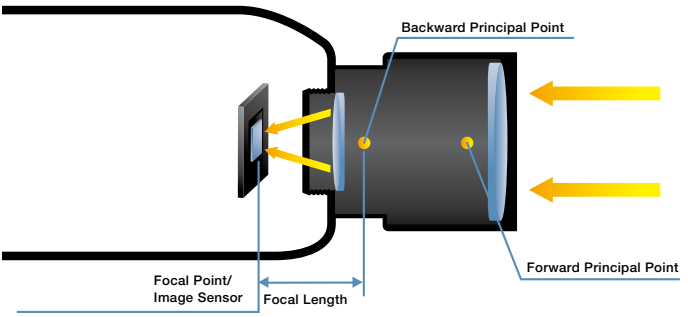


Figure 2.1 Focal length

The shorter the focal length, the wider field of view it offers and higher level of distortion it may cause. In contrast, the longer the focal length, the smaller viewing angle and field of object it has.

Figure 2.2 shows image distortion caused by a shorter focal length and the telephoto effect resulting from a longer focal length.

(a) (b) (c)

Figure 2.2 Comparison of images with (a) wide (b) normal (c) tele focal length

Lenses include the following types:

- **Fixed lens:** the focal length cannot be changed.
- **Vari-focal lens:** the focal length (field of view) can be manually adjusted;. The most common vari-focal lens is 3.5 - 8 mm.
- **Zoom lens:** a kind of vari-focal lens with motorized mechanism to adjust its focal length. Generally, AF (Auto Focus) algorithm is used to focus automatically.

Figure 2.3 Fixed and vari-focal lenses

2.1.2 Iris

Iris can control the amount of light entering the lens during exposure. Iris is one of the most important elements for light sensitivity, along with aperture, shutter time, sensor, and gain.

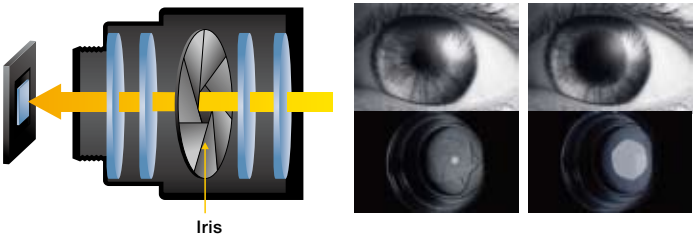


Figure 2.4 Iris in contrast to eye pupil

Iris is measured in F-number, which is the ratio of the focal length to the lens diameter. Iris size is inversely proportional to F-number. Every time the F-number increases towards a larger number, the exposure ratio will reduce by half (Figure 2.6).

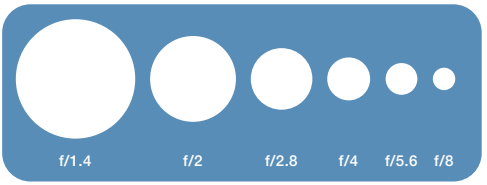


Figure 2.5 Relationship between F-number and aperture

F-number	1.4	2	2.8	4	5.6	8
Exposure ratio	32	16	8	4	2	1

Figure 2.6 F-number and corresponding exposure ratio

Iris includes the following types in terms of control methods:

Manual-iris

Manual-iris is adjusted with a ring on the lens. It is used when light sources are steady.

Auto-iris

Auto-iris can automatically adjust the amount of light entering with a mechanism to have a camera stay in an optimal light level. As a result, it is mainly required for outdoor applications or the places where lights change frequently.

There are two types of auto-iris: Video-drive iris and DC-drive iris.

- **Video-drive iris:** video signal is transmitted to a drive circuit in the lens and converted to currents to control the iris motor. Because the amplifier circuit is built in the lens, a Video-drive iris lens is more expensive.
- **DC-drive iris:** the iris is controlled by DC currents. Due to the drive circuit is integrated in the camera instead of in the lens, DC-drive iris lens features lower costs.

2.1.3 Lens Mount Types

C- and CS-mount are two major lens mount standards developed for the purpose of changing lens. The main difference between C/CS-mount lenses lies in the flange focal distance. The flange focal distance for a CS-mount lens is 12.5mm while 17.526mm for a C-mount lens (Figure 2.7). A CS-mount lens has higher cost efficiency and smaller size because fewer glass components are used.

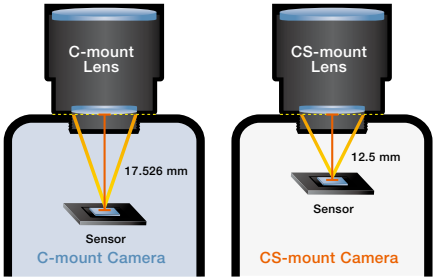


Figure 2.7 Comparison of focal distance for C/CS-mount lenses

Note that a C-mount lens can be used on a CS-mount camera by adding a 5 mm spacer (C/CS adapter ring), but a CS-mount lens cannot.

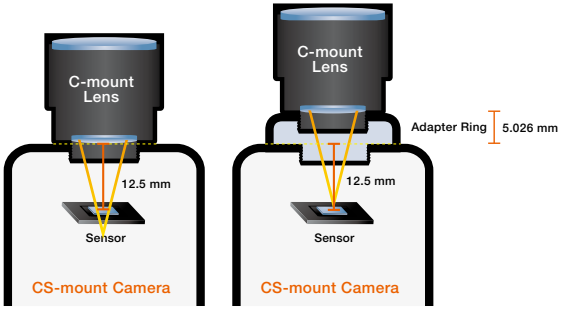


Figure 2.8 CS-mount camera with C-mount lens using adapter ring

VIVOTEK's IP7161 can fit in with either a CS-mount or C-mount lens by only adjusting an adjustment ring (Figure 2.9). The innovative method improves lens compatibility and installation.

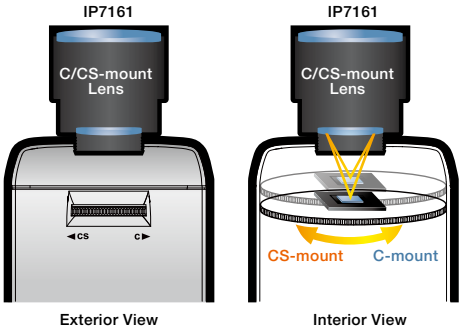


Figure 2.9 Operation of VIVOTEK IP7161's adjustment ring

2.2 Image Sensor

An image sensor plays a key role in converting lights through the lens into electrical signals. Based on the manufacturing process, there are two types of sensors: CMOS (Complementary Metal Oxide Semiconductor) and CCD (Charge-coupled Device).

2.2.1 Sensor Types

CMOS

CMOS is a standardized and constantly developing manufacturing process used in the semiconductors industry. Each pixel on a CMOS sensor is accompanied by an amplifier based on p-n junction structure. The p-n junction structure receives photons from the sensor and transmits them to an image signal processor.

CCD

CCD is a manufacturing process specially developed for digital imaging. A CCD is an analog shift register that enables the transportation of analog signals (electric charges) through successive stages (capacitors), controlled by a clock signal. The analog signals in each row of the capacitors are transmitted and converted to digital via an analog-to-digital IC.

Table 2.1 Comparison of features and environments for CMOS and CCD

	CMOS	CCD
Features	■ No artifacts, smear, or blooming ■ Low power consumption ■ Low cost	■ High light sensitivity ■ High color saturation ■ Low noise in low Lux
Environment	Widely used in indoor	Widely used in outdoor

2.2.2 Resolutions

Resolution refers to the number of pixels in a horizontal row and vertical column of an image. For example, a resolution of 1280x1024 means the horizontal row consists of 1280 pixels and the vertical column includes 1024 lines. The resolution of the entire image is thus around 1.3 megapixel pixels. The higher the resolution, the more information can be rendered, and thus the better image quality.

In traditional CCTV systems, the maximum resolution is 720x480 for NTSC (National Television System Committee) and 720x576 for PAL (Phase Alternating Line).The most commonly used resolution is 704x480 NTSC/704x576 PAL.

NTSC

As the world's first color TV broadcast standard, NTSC was developed by National Television System Committee in 1953. With an image size of 704x480 and up to 30 frames per second, NTSC is mainly adopted in the United States, Canada and Japan that uses 60Hz AC electricity.

NTSC signals can be displayed on a black-and-white TV because they contain luminance signals and color information. However, it has the disadvantages of phase distortion and unstable color.

PAL

1967 saw the development of a new color encoding standard for TV broadcasting in Germany, known as PAL, which was exclusively developed for the 50Hz AC electricity used in Europe. PAL has an image size of 704x576, with a full frame rate of 25 per second.

Since the phase of the color information in each line is reversed, PAL reduces color distortion problems.

D1

D1 format, also known as SMPTE 259M, is a digital image format developed by SMPTE Engineering Committee in 1986, and is used in tape recorders. In the NTSC system, D1 has an image size of 720x480, with maximum 30 frames per second; in the PAL system, D1 image size is 720x576, with maximum 25 frames per second. D1 format is commonly used by analog cameras.

CIF

CIF (Common Intermediate Format), frequently used in video conferencing, appeared for the first time in the ITU-T H.261 recommendation in 1990. CIF image size is 352x288, equal to 1/4 of a PAL image. Its full frame rate is 30 frames per second, the same as NTSC.

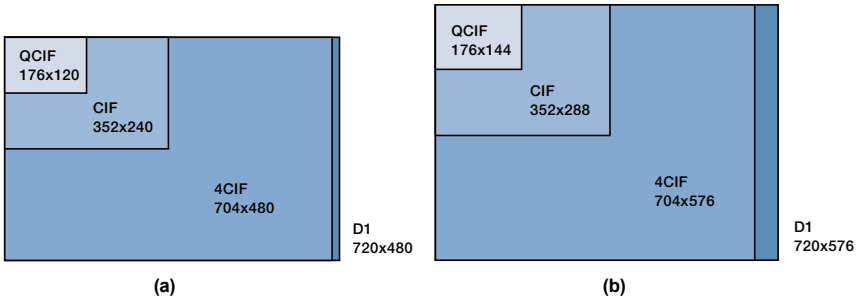


Figure 2.10 CIF for (a) NTSC and (b) PAL

VGA

VGA (Video Graphics Array) format was defined by IBM in 1987, with an image size of 640x480. Because a common standard for PCs and industrial monitors, VGA has been widely used in digital image devices. IBM has extended the VGA standard further into 1024x768 XGA (Extended Graphics Array) and 1600x1200 UGA (Ultra Graphics Array).

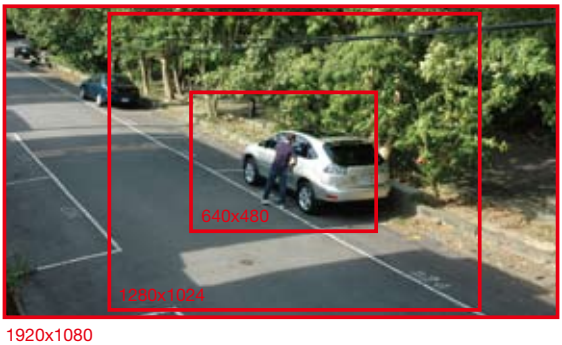


Figure 2.11 Comparison of image sizes for VGA, 1.3 MP and 2 MP

Megapixel

A megapixel network camera features a resolution at least three times larger than that of an analog CCTV camera.

A megapixel camera is mainly applied in occasions when accurate identification is needed such as vehicle license plate recognition or facial recognition for it can provide images with exceptional details. Because of its high number of pixels, a megapixel camera is also used in spacious areas such as parking lots or airports to provide images with a wide view.

The megapixel sensor has contributed to a new breed of non-mechanical PTZ cameras, known as digital PTZ cameras. The camera captures a megapixel image and delivers only a user-defined thumbnail to the monitor so that users can view different images by selecting on the monitor instead of physically moving the camera.

2.2.3 Sensor Scan Modes

Image sensor scan modes include interlaced and progressive scan.

Interlaced Scan

Interlaced scan split a scene into even and odd fields that contain even and odd lines, respectively. When rendering the entire scene, the even field is displayed first, followed by the odd field. The time interval between the appearance of the two fields will lead to jagged edges, especially for a moving object.

Interlaced scan is mainly used in TV monitors with a lower refresh rate, which causes the screen to flicker easily. Interlaced scan can reduce flickers because the field refresh rate of the interlaced scan seems two times faster than the original frame rate.

Some monitors solve jagged edges by dropping odd field and replicate the even field as the odd field. However, the vertical resolution will be cut by half.

Progressive Scan

Progressive scan renders the entire scene by displaying the even and odd lines of the frame sequentially instead of by field. Since there is no time interval between each display, the problem of jagged edges when displaying moving objects is eliminated.

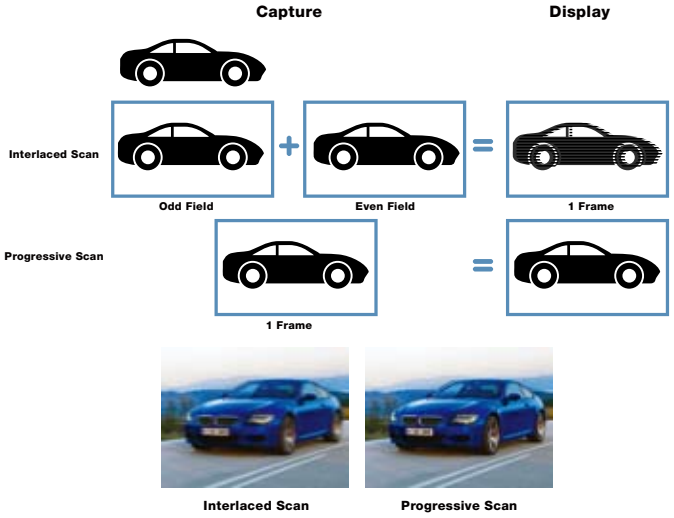


Figure 2.12 Progressive scan eliminates jagged edge artifacts of interlaced scan

With the refresh rate of a LCD monitors and a LCD TV enhancing to the same level of human eyes, there is no need to use interlaced scan to reduce screen flickers. Progressive scan is thus replacing interlaced scan and will become the mainstream scan technology.

2.2.4 Wide Dynamic Range

When shooting in high contrast, backlight, glare and light reflection environments such as the entrance, ATM or the window side, the object will appear dark and unrecognizable. WDR (Wide Dynamic Range) technology can ensure an identifiable image of all objects under such conditions by appropriately exposing the entire scene, both the darkest and brightest parts. VIVOTEK's award-winning IP7142 and FD7141 support WDR, enabling the camera to cope with challenging light conditions.

(a) (b)

Figure 2.13 Image quality (a) without WDR and (b) with WDR

2.3 Lens and Image Sensor Considerations

2.3.1 Lens Form Factors for Image Sensor

Sensor sizes are specified by the diagonal and mainly include 1/4", 1/3", and 1/2". A lens can fit in with a smaller sensor. When using with a larger-sized sensor, for example, a 1/4" lens with a 1/3" sensor, the situation of dark corners in the image will be caused.

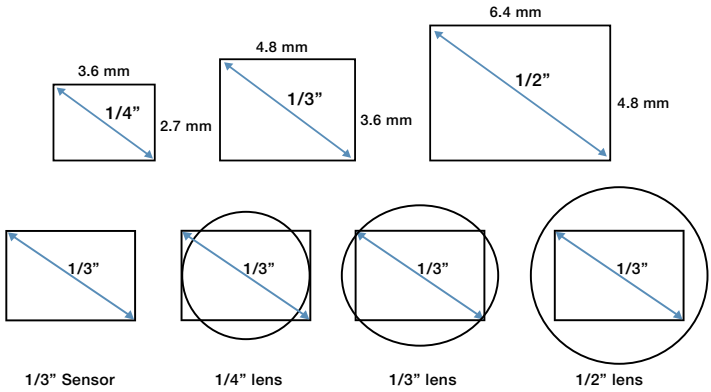


Figure 2.14 Sensor size and comparative lens size

2.3.2 View Angle

View angle is determined by the focal length of the lens and the sensor size. The shorter the focal length (Figure 2.15) and the larger the sensor size (Table 2.2), the wider the view angle.

Figure 2.15 View angle for different focal length with same sensor size

Table 2.2 View angle for different focal length with (a) 1/4" and (b) 1/3" sensors

Focal length	4 mm	6 mm	8 mm	12 mm
Vertical view angle	48°	33°	25°	17°
Horizontal view angle	37°	25°	19°	12°
Diagonal view angle	58°	41°	31°	21°

(a)

Focal length	4 mm	6 mm	8 mm	12 mm
Horizontal view angle	61°	43°	33°	22°
Vertical view angle	48°	33°	25°	17°
Diagonal view angle	73°	53°	41°	28°

(b)

2.3.3 Day and Night

Infrared light has a different wavelength from visible light, leading to jagged and blurred images. The day and night functionality can reduce the influence of infrared light on image quality and can be achieved by using an IR-cut filter removable and IR-corrected lens. During the daytime with sufficient illumination, infrared light is blocked to avoid color shift. During the night, infrared light can be utilized to enhance cameras' night vision so as to maintain good image quality.

ICR

An ICR (IR-cut Filter Removable) is a mechanical shutter design. It is placed between the lens and the image sensor and is controlled by a motor or an electromagnet (Figure 2.16).

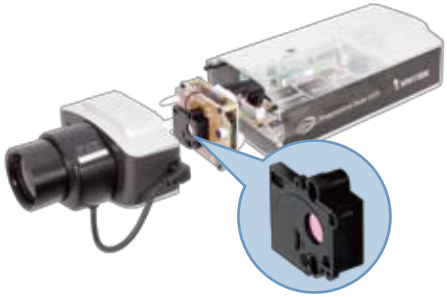


Figure 2.16 Placement of ICR

When the ICR is switched on, it will block infrared light and allow only visible light to pass through. When the ICR is switched off, infrared light will be allowed and images will turn into black-and-white mode, which is more sensitive to infrared light (Figure 2.17).

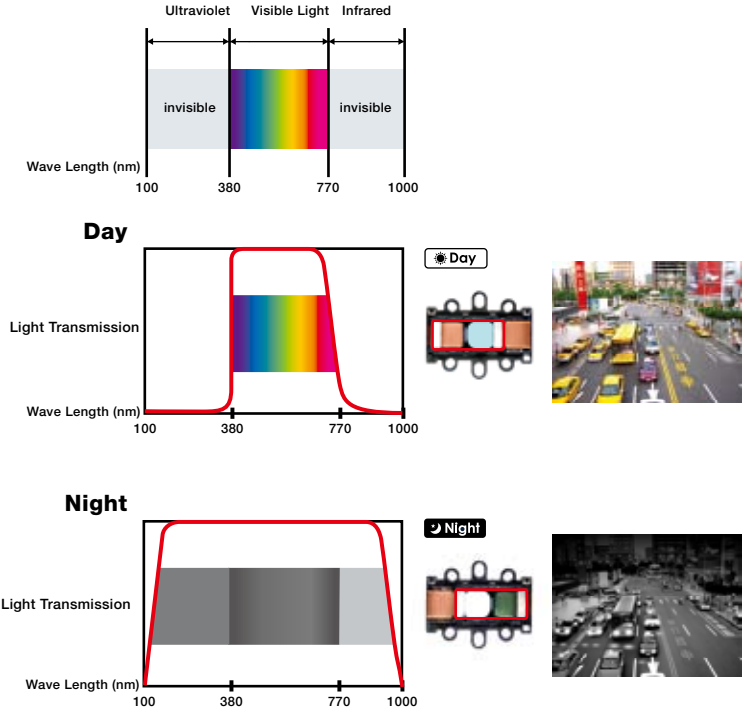


Figure 2.17 Operation of ICR in daytime and nighttime

IR Coating

Another way to block infrared light is to apply a coating on the lens; however, this will reduce light sensitivity of the lens in nighttimes.

IR Corrected

When the network camera is used on the visible light and infrared light, it is suggested to use an IR corrected lens with special optical design or materials to focus the visible light and infrared light on the same point (Figure 2.18).

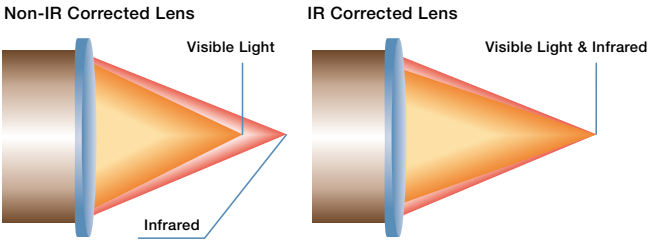


Figure 2.18 Focusing of visible and infrared light with non-IR and IR corrected lenses

In the daytime, images generated by an IR corrected and a Non-IR corrected lens are of identical quality (Figure 2.19. a). During the night, images generated by a Non-IR corrected lens become blurred, while those by an IR corrected lens remain clear (Figure 2.19. b).

IR corrected Lens (a) Non-IR corrected lens

IR corrected lens (b) Non-IR corrected lens

Figure 2.19 Image quality by IR-corrected and non-IR-corrected lenses in (a) daytime and (b) nighttime

IR LEDs

To get a clear image under poor-light environments, purchasing additional IR LED accessories or choosing network cameras with built-in IR LEDs will be required.

Chap.3
Video and Audio Compression

Compression technologies have a major impact on image quality, bandwidth usage, storage space and system loading. A high compression ratio can significantly reduce file size, and thus cut down bandwidth usage and storage space. However, a high compression ratio may cause a trade-off between bandwidth and image quality.

3.1 Video Compression

MJPEG, MPEG-4 and H.264 are three major video compression technologies used by the IP surveillance industry. Each technology has a different compression ratio and is intended for different applications and purposes.

3.1.1 MJPEG

MJPEG (Motion JPEG), announced by JPEG (Joint Photographic Experts Group) in 1992 and approved by ISO in 1994, is a multimedia format that compresses each video frame separately as a JPEG image. The technology is widely used in DSCs (Digital Still Camera) and other consumer electronics.

Technology

MJPEG compresses the entire image of each frame as a key frame, which is encoded and decoded independently without referring to the previous or sequential frames. This results in more redundancy in image size.

Figure 3.1 shows each frame is encoded separately by MJPEG, including the motions (the man's movement) and the still background (the car).

Figure 3.1 MJPEG encodes each frame entirely

Every encoded frame is independent from the previous or sequential frame (Figure 3.2).

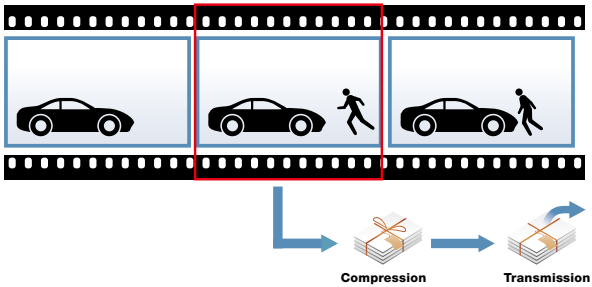


Figure 3.2 MJPEG encodes each frame independently

3.1.2 MPEG-4

MPEG-4 was formed by the MPEG working group under ISO and IEC in 1998. It was developed to facilitate video streams transmitting over the Internet and is mainly used for bandwidth-limited applications.

Technology

MPEG-4 is a video compression standard featuring more compression efficiency. Besides some key frames that are compressed entirely, MPEG-4 finds the differences from a reference key frame, leaves out redundant information and compresses only frame-to-frame differences. This significantly reduces file size and bandwidth requirements.

Figure 3.3 shows MPEG-4 encodes entirely the first frame, but only differences in the second and third frames.

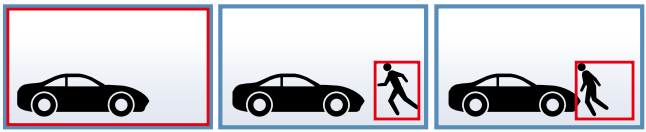


Figure 3.3 MPEG-4 encodes frame-to-frame differences

Figure 3.4 shows MPEG-4 finds and simply compresses the differences of two frames.

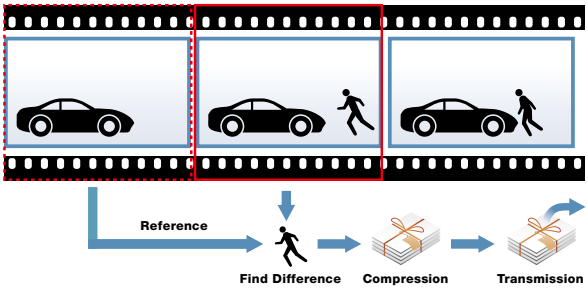


Figure 3.4 MPEG-4 refers previous frame to find differences

3.1.3 H.264

H.264 was initially developed by ITU (International Telecommunication Union) and then published by JVT, a group combined by ITU and ISO/IEC, in 2003. H.264 is also known as MPEG-4 part 10. H.264 has a higher compression ratio than MPEG-4, and thus can further reduce bandwidth usage.

Technology

Similar to MPEG-4, sequential and previous key frames are required during compression and decompression. H.264 provides a more efficient method of compression with more precise motion search and prediction; however, it requires more powerful CPU capability.

Table 3.1 shows H.264 has a higher compression ratio than MJPEG and MPEG-4, but its CPU loading ratio is also higher than the other two formats.

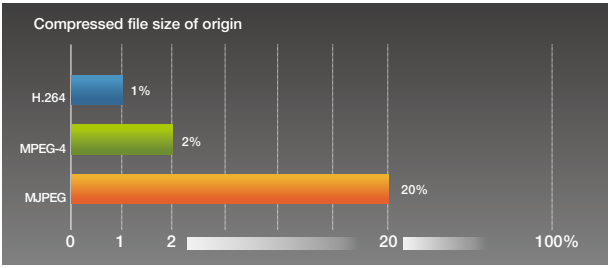


Figure 3.5 Compressed file size of MJPEG, MPEG-4 and H.264

Table 3.1 Comparison of MJPEG, MPEG-4 and H.264

	MJPEG	MPEG-4	H.264
Compressed file size	20%	2%	1%
Bandwidth comparison ratio	20 :	2 :	1
Encoding CPU loading ratio	1 :	4 :	10
Application	■ Local storage ■ Snapshot viewing	■ Moving picture viewing ■ Real-time transmission	■ Moving picture viewing ■ Real-time transmission

Table 3.2 shows H.264's bandwidth requirement is lower than MJPEG and MPEG-4 at the same frame rate.

Table 3.2 Bandwidth requirements by MJPEG, MPEG-4 and H.264

Bandwidth requirement in KByte	MJPEG	MPEG-4	H.264
CIF 30fps	302	45	27
VGA 30fps	819	123	75
1.3M 5fps	435	155	97

3.2 Audio Compression

Major audio compression technologies include G.711, AMR and AAC, which will be introduced below.

3.2.1 G.711

G.711 is a speech compression standard established by ITU in 1972, and is widely used for voice communications in the telecom industry, where audio quality is not the first priority.

G.711 has a bit rate of 64 kbps. Audio quality of this standard is quite low because signals may suffer from a heavy loss in digitization.

3.2.2 AMR

AMR (Adaptive Multi-Rate) was announced by 3GPP in 1998, a standard developed for mobile communications. Its compression ratio is better than G.711 and is widely applied to 3G mobile phones.

AMR bit rate ranges from 4.75 – 12.2 kbps. It offers a higher compression ratio and suffers from a slighter loss compared with G.711.

3.3.3 AAC

Announced in 1997, AAC (Advanced Audio Coding) is an audio compression standard based on MPEG-2. The standard is widely used in consumer electronics.

Table 3.3 indicates AAC for music playback purposes offers higher audio quality than G.711 and AMR aimed at voice communications.

Table 3.3 Comparison of G7.11, AMR and AAC

	G.711	AMR	AAC
Sample rate (Hz)	8K	8K	8K ~96K
Bit rate (bps)	64K	4.75K~12.2K	16K~320K
Application	General speech	3GPP speech	CD quality

3.3 Video and Audio Streaming

3.3.1 Multiple Streams

Multiple streaming allows each video stream to be delivered in a different resolution, frame rate, and image quality for individual quality or bandwidth demands. As a result, the camera can simultaneously transmit a small image in CIF format for real-time monitoring and a large megapixel image for storage. The CIF image can be directly displayed on the screen without much decoding or further scaling, thereby drastically reducing CPU loading. In addition, because different devices such as PCs and mobile phones have different requirements for image sizes, resolutions, and frame rates, multiple streaming gives users a higher level of flexibility for dealing with camera images on different platforms. (Figure 3.6).

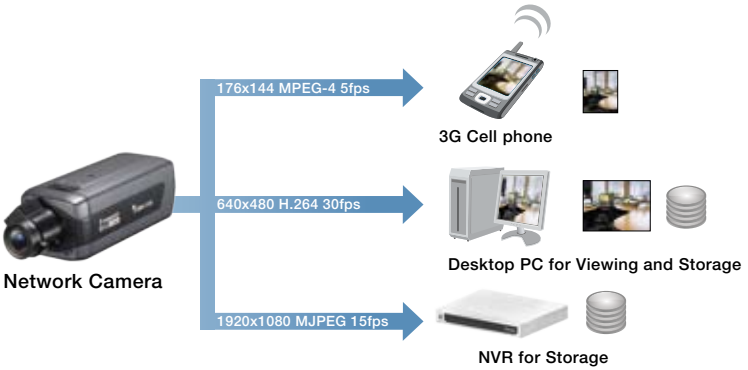


Figure 3.6 Multiple streams are sent with different configurations simultaneously

3.3.2 Two-way Audio

Generally, audio transmission methods consist of simplex, half duplex and full duplex. Unlike simplex and half duplex, full duplex provides simultaneous communications capability, also known as two-way audio.

Simplex

Voices can be transmitted in one direction only, from the sender to the receiver. For example, only the control site or the monitored site can make announcement; the receiver cannot make any response.

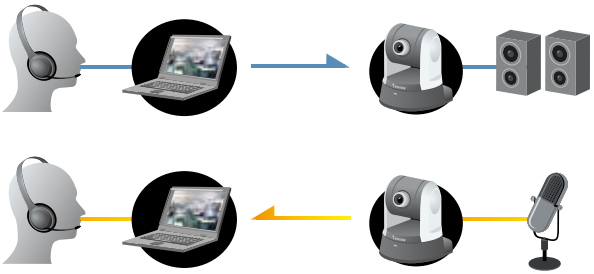


Figure 3.7 Simplex allows only unidirectional communications

Half duplex

Voices can be transmitted in both directions, from the sender or the receiver, but only one direction at a time (Figure 3.8).

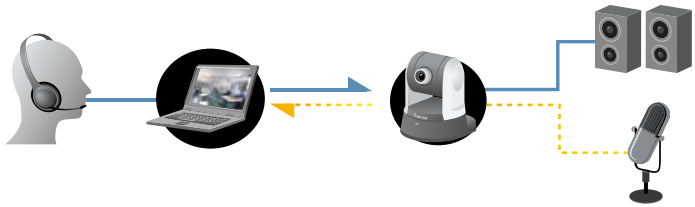


Figure 3.8 Half duplex allows communications in one direction at a time

Full duplex

Voices can be transmitted in both directions at the same time. As in Figure 3.9, the control site can speak to and receive voices from the monitored site. So does the monitored site.

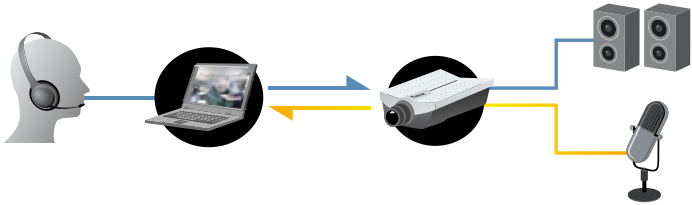


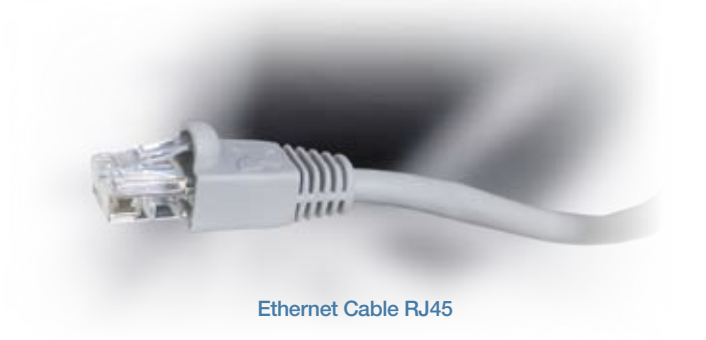
Figure 3.9 Full duplex allows communications in both directions at a time

Chap.4
IP Network

4.1 Network Types

As the most popular LAN technology, Ethernet uses a number of wiring to build the connection between end systems and the network. The most common type of Ethernet cables is RJ45. The original Ethernet transfer rate was 10Mbps. With bandwidth demand increasing, higher transfer rates such as 100Mbps, 1Gbps and 10Gbps were developed.

Currently, different Ethernet standards can be universally recognized as a form of “100BaseT”. The first number stands for the transfer rate and the last number or character indicates the characteristics of the transmission medium. For example, 100BaseT is 100 Mbps over network cable.



Ethernet Cable RJ45

4.2 Network Devices

Hub

A hub is a network device that connects a PC with an Ethernet cable to establish a LAN and enables the PC to communicate with other PCs on the LAN. When data is sent from a PC to a hub, the hub will duplicate the data to all PCs on the LAN. Only the destination PC will keep the data; other PCs will abandon the data.

Switch

A switch is a network device that serves the same purposes as hubs, but it makes more efficient use of bandwidth resources. A switch identifies the destination of data by its MAC address and sends it to the designated PC only, thereby reducing interference between data.

Router

A router connects different Ethernet networks to achieve network coverage. It can connect LANs that use different network protocols or transmission methods. When a router receives a packet, it checks the destination address of the packet, and designates an optimal path for it based on packet size and priority.

4.3 IP Address

Each network device has its own IP address. An IP address is like a doorplate of the device, helping data to be delivered to the correct destination. An IP address contains 32 bits, which are divided into four parts, each part separated by a dot, such as 255.255.255.0.

The following three blocks of the IP address space are reserved for private Internets (local networks):

- 10.0.0.0~10.255.255.255
- 172.16.0.0~172.31.255.255
- 192.168.0.0~192.168.255.255

However, with the number of network devices increasing, IP address shortage has become a problem. To solve the problem, DHCP and NAT and IPv6 were developed.

DHCP

DHCP (Dynamic Host Configuration Protocol) automatically assigns a valid IP address to a network device on the Internet. Allocating a fixed IP address for each device will result in idle IP addresses when the devices are not in operation. Therefore, DHCP can make more efficient use of the IP addresses.

NAT

NAT (Network Address Transfer) uses translation tables to change a private IP address of an outgoing packet from a client PC into a public IP address. In this way, multiple PCs can access the Internet through one public IP address.

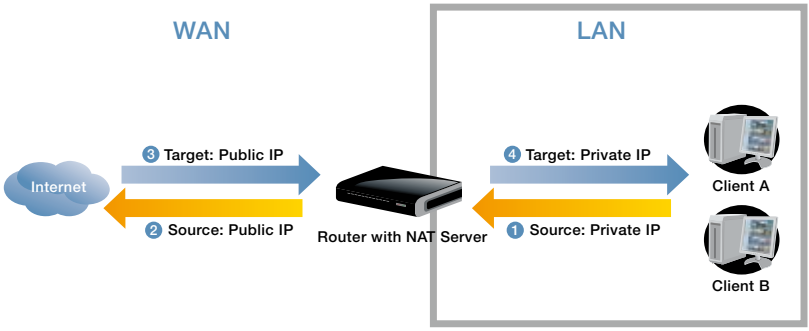


Figure 4.1 NAT enables multiple PCs to share one public IP address

NAT breaks the rule of one IP address for one network device. As a result, when multiple network devices are transmitting a great deal of data simultaneously, serious delay and packet loss may occur.

IPv6

IPv6 standard consists of 128 bits, which are divided into eight parts, each group containing four 16-bit digits and is separated by a colon. IPv6 IP addresses are presented in a different format from IPv4, for example 3ffe:0305:0000:0000:0000:0000:0000:0001.

Table 4.1 Comparison of IPv4 and IPv6

Feature	IPv4	IPv6	Comparison
Address space	32 bits	128 bits	IPv6 provides larger address space
Configuration setting	Manual	Auto	IPv6 doesn't need an independent DHCP
Priority control	No	Yes	IPv6 achieves higher video quality
Authentication	No	Yes	IPv6 provides safer data transmission

4.4 Network Protocols

Protocols are a set of rules that enable applications or devices to communicate with each other, allowing data to be transmitted and received accurately.

4.4.1 Device Connection

This section introduces two types of protocol, one for facilitating network connectivity after the device obtains a valid IP address and the other for building connection between networking devices and the Internet. The first type includes DNS and DDNS and the second type includes PPPoE and UPnP.

DNS

When locating a network device, you need to input a numerical IP address, which is difficult to remember. DNS (Domain Name System) allows you to input an IP address in text format and automatically maps it to the numerical IP address of that network device. For example, when a user inputs a registered domain name (such as www.vivotek.com), the DNS server automatically maps the domain name to an IP address such as 203.160.252.248.

DDNS

DDNS (Dynamic DNS) automatically matches a floating IP address to a registered domain name, allowing users without a fixed IP address to easily connect to a network device. For example, if you register a domain name as john-1.safe100.net, and the IP address for the first time connection is 203.160.252.200; the DDNS server will match it to john-1.safe100.net. Next time the device is online with a different IP address, such as 203.160.252.201, the DDNS will still match it to john-1.safe100.net. In this way, users only need to remember the registered domain name to locate your network device (Figure 4.2).

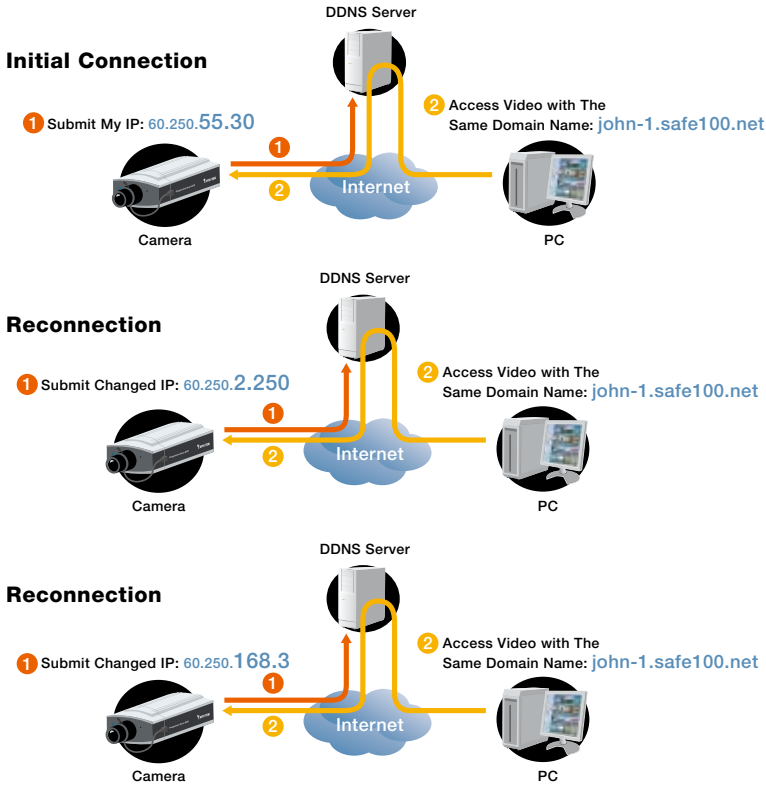


Figure 4.2 DDNS in operation

Figure 4.3 VIVOTEK DDNS server

PPPoE

PPPoE (Point-to-Point Protocol over Ethernet) is a protocol that enables connections between a DSL modem and the Internet. This service is provided by ISP (Internet Service Provider).

UPnP

UPnP (Universal Plug and Play) includes two main functions, UPnP port forwarding and UPnP presentation.

UPnP port forwarding enables network devices to easily communicate with each other over the Internet. When both the network device and router support UPnP, video streaming ports will be forwarded, so called port forwarding (Figure 4.4).

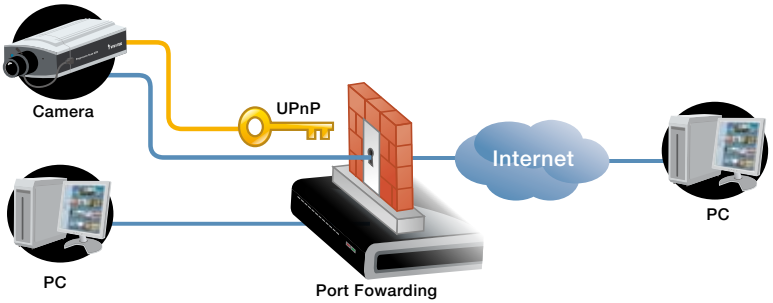


Figure 4.4 UPnP port forwarding

If the user's PC supports UPnP presentation, an icon of the network devices on the same LAN will appear in My Network Places to allow for direct access (Figure 4.5).

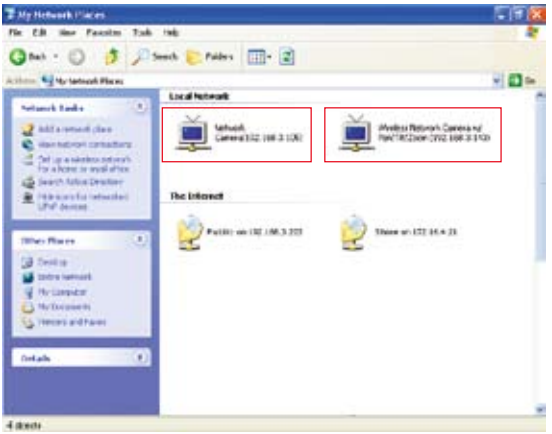


Figure 4.5 UPnP-enabled network cameras shown in My Network Places

4.4.2 Transmission Protocols

This section introduces two types of protocols. UDP, TCP and HTTP are underlying protocols that carries the data. RTSP/RTP/RTCP are real-time media transmission protocols.

● Data Transmission

UDP

A UDP (User Datagram Protocol) source port sends out packets continuously and does not require the destination port to return a confirmation message, allowing for more real-time audio and video streams. However, the packets may be lost due to network burst traffic and images may be broken. UDP connection is mainly used for time-sensitive responses and when the video quality is less important.

TCP

A TCP (Transmission Control Protocol) source port sends out packets and waits for a confirmation message from the destination port before sending out sequential packets. If no confirmation message is received, the source port will send that packet again. TCP guarantees the complete delivery of streaming data and thus provides better video quality. Nevertheless, its real-time effect is inferior to UDP.

HTTP

Designed for users to view information on a web page through a browser, HTTP (Hypertext Transfer Protocol) allows the same quality as TCP protocol without needing to open specific ports for streaming under some network environments. Users inside a firewall can utilize this protocol to allow streaming data to come through.

● Media Transmission

RTSP

RTSP (Real Time Streaming Protocol), which consists of RTP and RTCP, is a protocol used to facilitate multimedia streaming over the Internet. As a protocol for 3GPP streaming, RTSP enables users to access video images via a 3G phone.

4.4.3 Video Transmission Methods

Unicast

With unicast, data is transmitted to the designated PC only and other PCs on the same network will not receive the data. If more than one PC request for the same piece of data, the source PC has to send the data repeatedly to different destinations. This is the most popular transmission method and is also known as One-to-One transmission.

Broadcast

Broadcast is mainly used on the LAN. Compared with unicast, all network devices in broadcast on the same network will receive data whether they need it or not. The source PC sends data to a router where data is replicated and sent to multiple destination PCs requesting for the same data. It is also called One-to-All transmission.

Multicast

With multicast, data is transmitted to a multicast group consisting of PCs requesting for the same data on the Internet. Once the data reaches the multicast group, it is duplicated and delivered separately to each PC in that group.

Multicast significantly reduces bandwidth usage and is suitable for web video applications such as VoD, e-learning and video conferencing. It is also called One-to-Many or Many-to-Many transmission.

4.4.4 Event Notification

SMTP

SMTP (Simple Mail Transport Protocol) is for e-mail transmission. With SMTP, e-mail can be transmitted from the client to the mail server.

FTP

FTP (File Transfer Protocol) is for file transmission. FTP allows you to upload and download files to and from a server. Via FTP, the user can upload information from a network camera such as snapshots or video clips to a FTP server when an event occurs.

4.4.5 Timing Correction

NTP

NTP (Network Time Protocol) synchronizes the system time of a network device on the Internet to a reference time. After a network device sends a request to a NTP server for time synchronization, it will receive a Greenwich Mean Time returned from the server. NTP can solve the time difference between network cameras and other network devices.

4.4.6 Video Quality Control

QoS

For bandwidth limitation applications, it is important to manage bandwidth allocation carefully. As part of the IEEE 802.1p standard, QoS (Quality of Service) aims to optimize bandwidth usage. QoS ensures streaming performance at a steady level by transmitting data according to its priority and by the requests of the applications. With QoS, bandwidth resources are used more efficiently and real-time multimedia streams can be transmitted constantly. VIVOTEK products support QoS to allow for optimized bandwidth efficiency.

In a non-QoS environment, bandwidth is likely to be occupied by data stream, leading to jittering of other video streams (Figure 4.6.a). In a QoS environment, since bandwidth allocation is optimized, every video stream can be transmitted smoothly in priority (Figure 4.6.b).

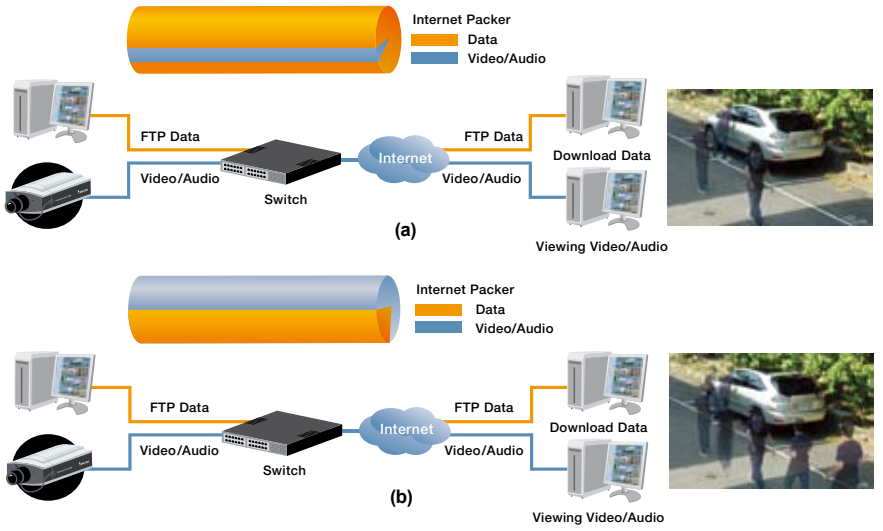


Figure 4.6 Bandwidth allocation for (a) non-QoS, (b) QoS

4.5 Wireless Networks

Wireless technologies include WiFi, WiMAX and 3GPP. WiFi is used for short-distance transmission while WiMAX for long distance.

4.5.1 WiFi

IEEE 802.11, developed by the IEEE LAN/MAN Standards Committee, is a set of standards for wireless local area network computer communication. 802.11b, 802.11g, and 802.11n are widely used in wireless network devices.

802.11b

802.11b operates in the 2.4GHz band with a transfer rate of 11Mbps and a range of 35 meters indoors and 100 meters outdoors. The drawback of 802.11b is that signals can be blocked by walls. The 2.4GHz is also subject to interference caused by electronics or Bluetooth signals.

802.11g

802.11g, the same as 802.11b, operates in the 2.4GHz band. It has a transfer rate of 54Mbps, similar to that of 802.11a, and a range of 25 meters indoors and 75 meters outdoors. 802.11g has the same weaknesses as 802.11b; however, it outperforms 802.11b in transfer rate.

802.11n

802.11n is a wireless standard certified in 2008. Based on MIMO (Multi-input Multi-output), 802.11n boasts an amazing transfer rate of 600Mbps and a range of 50 meters indoors and 300 meters outdoors. It can operate in the 2.4GHz or 5GHz band and is ideal for applications demanding high bandwidth such as high-definition video streaming.

4.5.2 3GPP

3GPP is a set of open standard protocols for audio and video bitstreams to be viewed on a 3G mobile phone (Figure 4.7). This standard is widely supported by major mobile phone vendors.

All of VIVOTEK's 7000-series or above network cameras provide 3GPP support, allowing users to access video images at any time and anywhere via a 3G mobile phone.

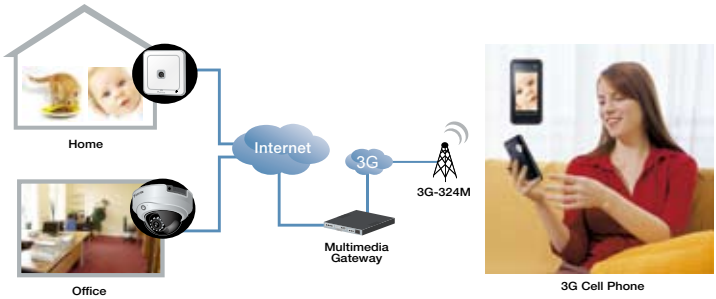


Figure 4.7 Mobile surveillance via 3GPP

4.5.3 WiMAX

WiMAX is a wireless broadband technology featuring long-distance transmission capability. It is an alternative to cable networks such as ADSL in remote areas where network infrastructure is incomplete.

WiMAX, developed by the 802.16 group of IEEE, is also called the 802.16 standard. WiMAX offers a transfer rate of 70Mbps in a range of 70 kilometers, making it ideal for long-distance and outdoor connection. Compared with 802.11X standards, WiMAX provides wider coverage, a higher transfer rate, a larger transmission volume and higher QoS.

4.6 Security

Since data is likely to be intercepted during transmission, appropriate protection schemes are needed. The following methods can protect data from security risks.

4.6.1 IP Filtering

You can confine a client's IP address within a specific range to authorize or deny user access. A client's IP address in an authorized list will be able to access data while that in a denied list will be refused to access.

4.6.2 Username and Password

You can assign accounts and passwords to users so as to achieve simplified and efficient management. VIVOTEK offers the three user privilege levels of administrator, operator and viewer; only administrators can make configurations.

4.6.3 Security Protocols

Security protocols protect data from unauthorized access. SSL/TLS and IPSec are three basic network security protocols. The major difference is that SSL/TLS encrypts the data and IPSec encrypts the transmission channel.

SSL/TLS

SSL (Secure Sockets Layer) encrypts data transmitting between the server and the client to ensure the confidentiality and integrity of the data. When a client submits a request for accessing web pages, a public key is sent to the client for data encryption. Data encrypted by the client using the pubic key can be decrypted only by the server's private key. Due to this property of the keys, the client is able to send secure data that can be understood only by the server. SSL can protect data from being counterfeited, intercepted or tampered and is the most common security standard for e-commerce.

TLS (Transport Layer Security) is a standard developed on the basis of SSL for higher security, confidentiality, data integrity and authentication.

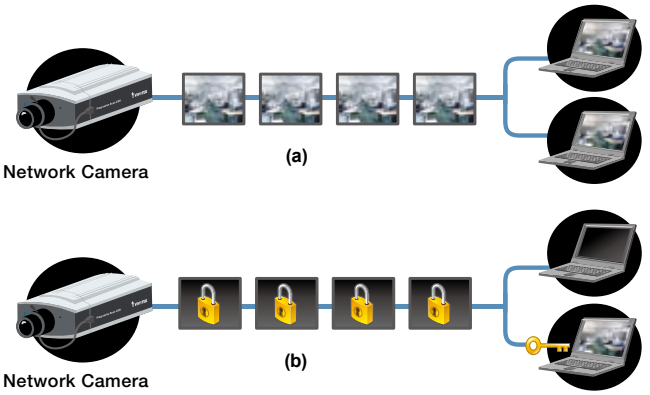


Figure 4.8 Data transmission (a) without SSL/TLS encryption and (b) with SSL/TLS encryption

HTTPS

HTTPS is a combination of HTTP and SSL/TLS. It encrypts data at the source port and decrypts it at the destination port. HTTPS is mainly used to protect e-commerce, asset management, e-mails or IP surveillance systems.

IPSec

IPSec (IP Security) is a security protocol designed to protect communications over the Internet. Incorporating security protocols in IP architecture can ensure network communications security, even if the data is not encrypted with SSL/TLS.

IPSec provides two functions, authentication and confidentiality. The authentication function confirms the identity of the source and the destination PCs so as to protect data transmitting between them. The confidentiality function encrypts the content to prevent from interception by the third party. Both authentication and confidentiality operate on the basis of encryption (or hashing). IPSec also provides regulations on key exchange to help generate and manage keys for encryption.

IPSec creates a secure network communications tunnel, such as VPN (Virtual Private Network). VPN builds transmission tunnels between two nodes on the Internet, rather than using physical cables for data transmission.

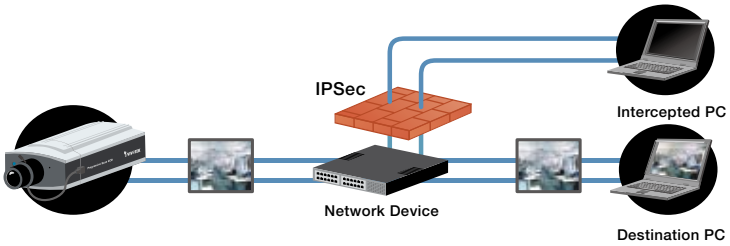


Figure 4.9 Encryption of transmission tunnels with IPSec

4.6.4 Security Wireless Transmission

WEP

WEP (Wired Equivalent Privacy), also known as Wireless Equivalent Privacy, is designed to protect data on a wireless network because data transmitted by radio wave can be easily intercepted. A key must be set in the wireless access point and when a user connects to the access point, he has to enter the same key to connect to the Internet. WEP can provide a security level comparable to cable networks.

WEP encrypts data from wireless access points with a shared key that contains 40 to 256 bits. The longer the key, the more difficult it is to crack, and the higher security it offers.

WPA

With the increasing computing capability of a PC, WEP, which uses a fixed encryption key, becomes vulnerable to be attacked. Hence, the Wi-Fi Alliance developed WPA (Wi-Fi Protected Access) /WPA2 standard based on WEP.

WPA uses TKIP (Temporal Key Integrity Protocol) that dynamically changes the key for each packet during transmission. With a 128-bit key, WPA offers a higher level of security than WEP. WPA provides data protection via user authentication, encryption and packet inspection. It also improves wireless network management. WPA2 indicates compliance with an advanced protocol that implements the full standard. In addition, WPA defines the use of AES (Advanced Encryption Standard) as an additional replacement for WEP encryption.

Figure 4.10 Encryption of data with WEP/WPA

4.7 PoE

Conventional network cameras require a power cable for power supply and an Ethernet cable for data transmission. PoE (Power-over-Ethernet), developed by the IEEE802.3af task force, enables power to be supplied over the same Ethernet cable, and thus eliminates the use of power cables. By connecting a PoE-supported camera to a PoE switch, you need not deploy additional power cables (Figure 4.11).

A PoE switch can provide 48 volts of direct current over two out of four pairs on an Ethernet cable, with maximum current of 400mA and maximum output power of 15.4W. IEEE has developed a new IEEE 802.3at standard, known as PoE+ to provide maximum output power of 30W.

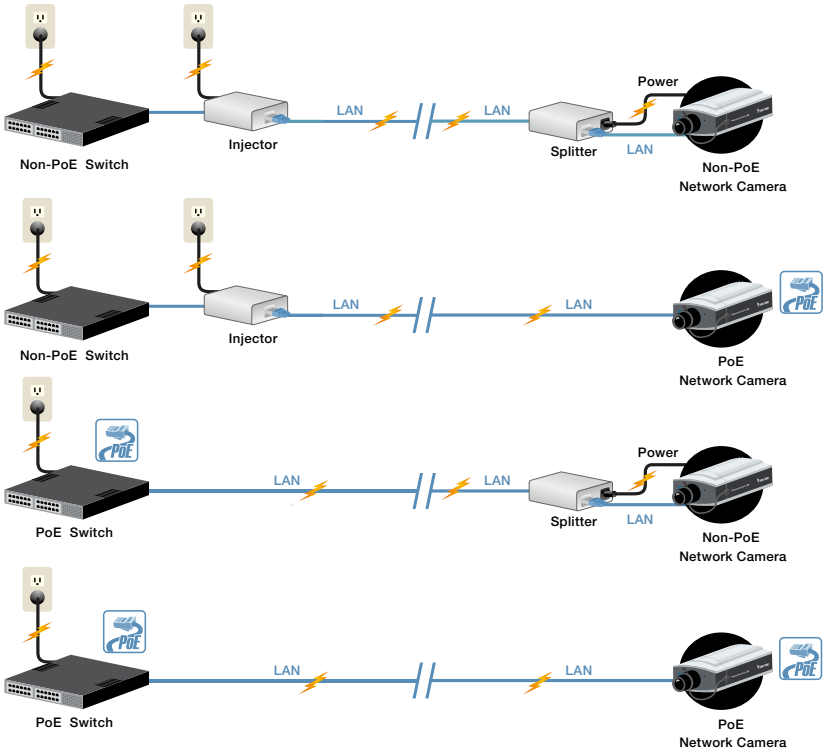
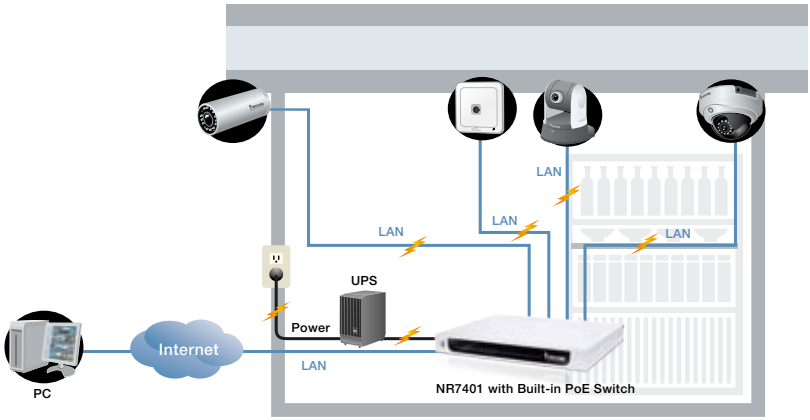


Figure 4.11 Connection of PoE and non-PoE network cameras



Retail Store

Figure 4.12 PoE-enabled devices for retail application

Chap.5
Camera Housing and Mounting

5.1 Housing

A housing protects cameras from damages caused by vandalism or harsh environments, thereby ensuring constant operation. Two major types of housing are vandal-proof and weather-proof housing.

5.1.1 Vandal-proof

A vandal-proof housing can resist violent attacks, enabling cameras to operate in high-risk public environments such as prisons, transportation stations, parking lots, and ATM sites. A vandal-proof housing features a robust design made of metal or polycarbonate plastic and can resist a violent impact force.

5.1.2 Weather-proof

A weather-proof housing protects cameras from damage caused by rain and dust, allowing cameras to be used outdoors. In extremely warm or cold environments such as in the desert or in snowy weather, a housing with a built-in heater and fan will be needed to ensure constant camera operation.

A weather-proof housing should conform to the IP rating that defines protection against solid objects and liquid on a six and eight scale respectively. Generally, a housing should be at least IP66-rated to provide sufficient protection for camera components.

Figure 5.1 Vandal-proof housing

Figure 5.2 Weather-proof housing

Table 5.1 Degree of protection against dust represented by first digit of IP rating

Prevents device from accessing hazardous parts	
0	Non-protected
1	Protected against solid foreign objects 50 mm diameter and larger
2	Protected against solid foreign objects 12.5 mm diameter and larger
3	Protected against solid foreign objects 2.5 mm diameter and larger
4	Protected against solid foreign objects 1.0 mm diameter and larger
5	Dust Protected
6	Dust-tight

Table 5.2 Degree of protection against water represented by second digit of IP rating

Prevent the damage of penetration of water into the housing	
0	Non-protected
1	Protected against drips
2	Protected against drips if the housing is bent at an angle of 15°
3	Protected against spray-water
4	Protected against splash-water
5	Protected against jet-water
6	Protected against strong jet-water
7	Protected against the effects of temporary submersion in water
8	Protected against the effects of permanent submersion in water

5.1.3 Covering

The two main types of coverings are transparent and smoke. A housing with a smoke cover makes the camera's shooting direction invisible and can be used if people feel uneasy with the perception of the cameras pointing at them.

5.2 Mounting

Due to demand for placing network cameras at different locations, you can choose different kinds of mounting solutions or mounting kits to solve the difficulties you may encounter. Different types of mounting can also provide different level of protection for cameras.

Figure 5.3 Mounting methods

Tamper-resistant Mounting

Tamper-resistant mounting is used to prevent ill-intentioned disassembly, enabling cameras to operate in high-risk public environments. The covering is fixed from the inside using tamper-proof mounting screws.

Figure 5.4 Tamper-proof mounting screws

5.3 Scanner

A network camera with a RS-232/422/485 interface can be connected to a pan/tilt scanner. With the scanner, a fixed network camera can change shooting direction, providing wider coverage.

Figure 5.5 Scanner

Chap.6
Bandwidth and Storage

6.1 Bandwidth Management

In order to achieve efficient video transmission, it is important to evaluate your bandwidth requirements before setting up an IP surveillance system.

6.1.1 Assessing Demands

Bandwidth requirements vary with the following factors.

- **Resolution:** the higher the resolution, the more bandwidth is required
- **Complexity of the scene:** the more complicated the scene, the more bandwidth is required
- **Compression type:** the lower compression ratio, the more bandwidth is required
- **Image quality:** the higher image quality, the more bandwidth is required
- **Frame rate:** the higher frame rate, the more bandwidth is required

6.1.2 Calculation

To assess bandwidth requirements, you can use Calculator.exe to evaluate the number of packets sent. You can download the file from http://www.vivotek.com/downloadfiles/faq/audiovideo.

6.2 Storage

Besides bandwidth assessment, your storage space is also required to be evaluated, especially with megapixel images.

6.2.1 Assessing Demands

The following factors must be taken into account when assessing storage demand:

- The number of cameras deployed
- Recording time
- Recording criteria, such as constant, scheduled or event-triggered recording
- Other factors such as codec, image quality and frame rate

Figure 6.1 will demonstrate the calculation of storage space required for one-day continuous recording with an assumed transfer rate of 400kbps. Note that 1 byte equals 8 bits and 400Kb totals 50KB (b refers to bit and B refers to Byte).

In the case of recording for 30 consecutive days, 8 hours per day, you should prepare at least 43.2GB (Figure 6.1).

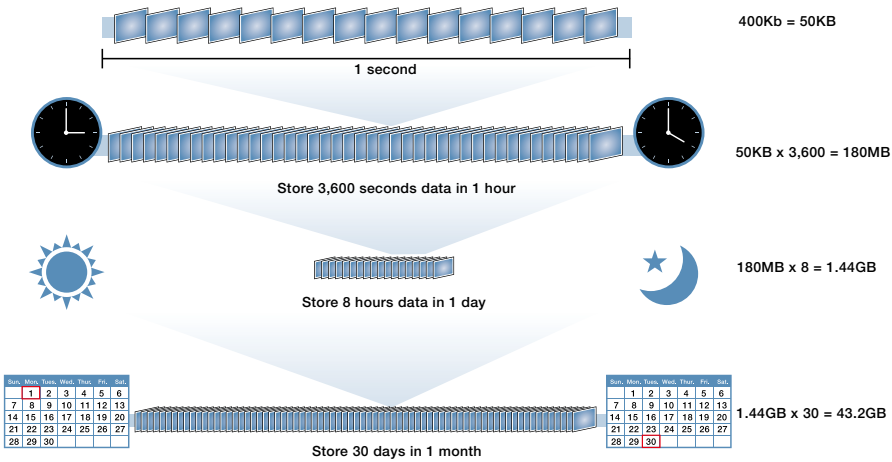

400Kb = 50KB
1 second
50KB x 3,600 = 180MB
Store 3,600 seconds data in 1 hour
180MB x 8 = 1.44GB
Store 8 hours data in 1 day
1.44GB x 30 = 43.2GB
Store 30 days in 1 month

Figure 6.1 Calculation of storage space required for 30-day recording (400Kb)

6.2.2 Storage Media

Various types of storage media have been developed to meet different demands and purposes, such as

- Internal buffer
- External memory cards
- DAS (Direct Attached Storage)
- NAS (Network Attached Storage)
- SAN (Storage Area Network)

Internal Buffer

A network camera is equipped with an embedded flash memory or DRAM as a buffer zone that enables temporary storage of pre- and post-event video images. Images are stored in the buffer zone for a short period of time before being transmitted to the back-end recording platform.

External Memory

CF, SD and SDHC cards are three main external memory types. They are designed for pre- and post-event storage and data portability. Many of VIVOTEK products are furnished with a SD/SDHC card slot for on-board storage.

DAS
Images are transmitted from a camera to a host PC via Ethernet cables and stored directly in the hard disk drive of the PC. DAS is aimed to enable storage and playback on the same PC and is mainly used by small- or medium-sized businesses.

NAS
Images are transmitted to a purpose-built NAS server via Ethernet cables for storage. NAS allows storage and playback on different platforms and is especially suitable for enterprises that need to access and share large-volume data

SAN
Images are sent to a purpose-built SAN server via an exclusive fiber optic cable for storage. As with NAS, storage and playback of images can be performed on different platforms, but SAN further reduces Ethernet bandwidth usage and offers a faster transfer rate.

6.3 Redundancy

In a bid to avoid significant losses from network downtime and hard disk drive cracks, it is highly recommended to plan a redundancy solution ahead, such as using back-up cables or RAID structure.

6.3.1 Cables

Additional cables can be deployed during installation for failover. When the trunk cable is out of order, system will switch over to the redundant cable to avoid system downtime.

6.3.2 RAID

RAID (Redundant Array of Independent Disks) is an array of several hard disk drives that can be used as one single hard disk drive. Data can be spanned over multiple disk drives under one system. If one of the drives cracks, the data can still be recovered.

The only difference between RAID and a hard disk drive is their array structure. Compared with a large-volume hard disk drive, RAID provides higher reading/writing speed, stronger data integration, redundancy and processing capability and better recovery capability.

RAID 0 (Striped)
With RAID 0, data is split into several segments and written to individual hard disk drives sequentially. For example, 256k data is split into four 64k segments and written to four hard disk drives.

RAID 0 can deliver better I/O performance and faster reading and writing speed. However, if one of the hard disks cracks or if any problem occurs, all data will be destroyed.

RAID 1 (Mirrored)
RAID 1 writes data simultaneously into two disk drives, one with the original data and the other with the duplicated copy. When one of the disk drives is out of order, users can still retrieve data from the other drive.

RAID 1 offers faster reading speed and better data; however, an additional drive must be added to store replicated data, thereby increasing installation costs.

RAID 5 (Parity RAID)

RAID 5 consists ists of at least three hard disk drives. Similar to RAID 1, RAID 5 stores redundant data in separate disk drives, but in an even- and odd-parity scheme. The parity is used for data recovery.

RAID 5 is more cost-effective than RAID 1 because only one drive is used to store parity. However, its writing speed is slower since at least two hard disk drives are needed when writing data (one for storing data, the other for storing parity) and its data security is more inferior. In addition, RAID 5 offers higher security than RAID 0 because parity can be used to restore data if a drive cracks.

Table 6.1 Comparison of RAID 0, RAID1 and RAID 5

RAID type	No. of hard disk drives required	Total storage space	Performance	Security	Main application
RAID 0	> 2	Capacity of all drives	High	Low	Users that require high performance
RAID 1	2	Capacity of half of the drives	Medium	High	When data security is top priority
RAID 5	> 3	Capacity of total minus one drive	Fast reading and slow writing speed	Medium	Ensuring uncompromising data security with limited budget

Chap.7
Video Management

Apart from network cameras, a successful IP surveillance system must include powerful central management software to achieve reliability, flexibility, scalability and high efficiency. Video management software provides basic monitoring, recording and management function as well as advanced functions such as intelligent surveillance and integration with other systems.

7.1 Video Management Platforms

There are two types of video management platforms: PC- and NVR-based.

7.1.1 PC-based

A PC-based platform is implemented by installing video management software on a PC or server, a standard hardware component. Before the installation, users have to figure out the system requirements such as CPU capability and operating system so as to achieve the expected performance. Since it is easier for users to operate, upgrade, integrate, most large organizations, institutes, or enterprises build up their surveillance systems by adopting PC-based platforms, integrated with IT or MIS management. As a result, many advantages such as scalability, integration, and flexibility are all included.

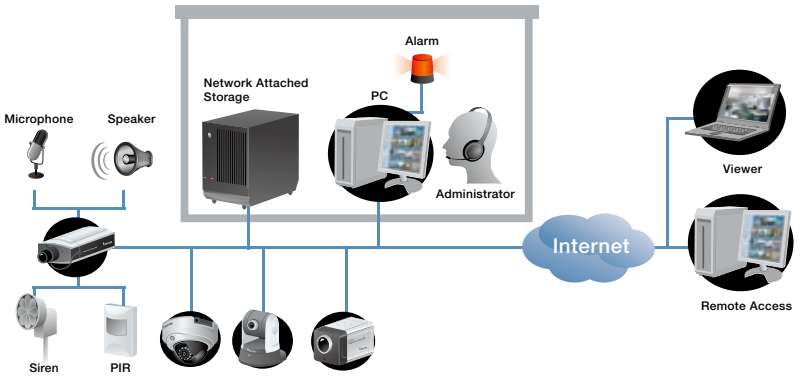


Figure 7.1 PC-based video management platform

VIVOTEK provides application software together with the package to help users set up an IP surveillance system with ease. From the application software, Installation Wizard 2 and PC-based central management software ST7501 are included.

Installation Wizard 2 is the new generation of VIVOTEK's installation software, in which the embedded intelligent functions will guide users to set up a network camera with ease. In other words, its "smart mode" enables those who has not much technical knowledge to be capable of installing a network camera themselves only by a few "clicks." It can automatically detect users' networking environments and help them get rid of some complicated setting inputs like IP Address, DDNS, UPnP Port Forwarding, and PPPoE connecting. Then, users may quickly connect their network cameras over the Intranet or Internet without any other advanced settings. From now on, the Installation Wizard 2 is free bundled along with VIVOTEK's packages. Therefore, you can enjoy all the benefits without any additional investment.

Figure 7.2 VIVOTEK Installation Wizard 2

As for ST7501, the functionalities will be introduced in section 7.2. VIVOTEK has formed an alliance with numbers of central management software development vendors in order to better fulfill customers' needs. For more information, please go to Alliance page on VIVOTEK website.

7.1.2 NVR-based

An NVR is a standalone recording device, in which video management software is pre-installed, providing easy-to-use interface and video management platform. It functions as a DVR with a network interface for the connection of a set of network cameras. However, unlike PC-based, an NVR does not allow changing or upgrading components, nor does it allow for the installation of additional applications. Due to limited scalability and compatibility, this platform is widely adopted in small- and medium-sized surveillance systems.

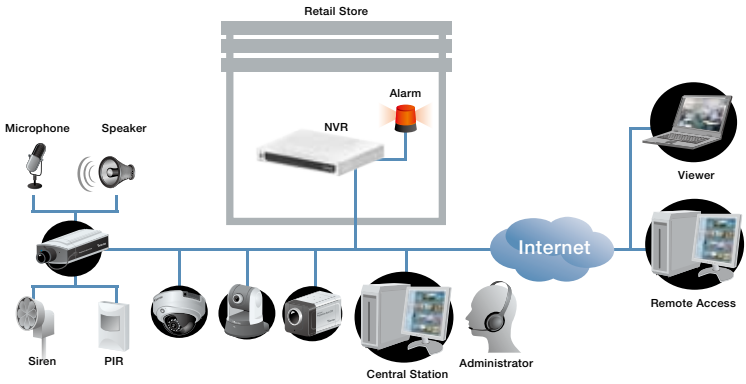


Figure 7.3 NVR-based video management platform

7.2 Basic Features of Software

Video management software mainly includes web-based software and central management software. Web-based software is built in the camera, allowing users to perform basic functions such as recording, monitoring and configurations. Relatively, central management software offers more powerful functions such as playback, remote monitoring in multiple monitors etc., to achieve efficient, flexible video management.

7.2.1 Monitoring

Users can view live video images with a web browser such as Internet Explorer, on a mobile device or via software (Figure 7.4). More than one users can access the camera to view the images at the same time.

Figure 7.4 Monitoring on different platforms

Through the management software, users can use different viewing modes like split windows to simultaneously view the transmitted images from multiple cameras.

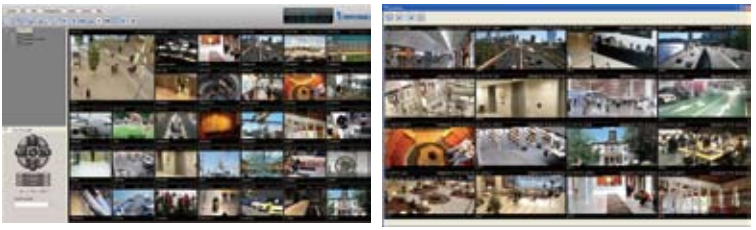


Figure 7.5 Dual-screen support of ST7501

7.2.2 Recording

Recording can be performed in different modes such as continuous, on schedule or on event trigger according to their needs. On-schedule or event-triggered recording is highly needed because the storage requirements will be reduced; so is the bandwidth.

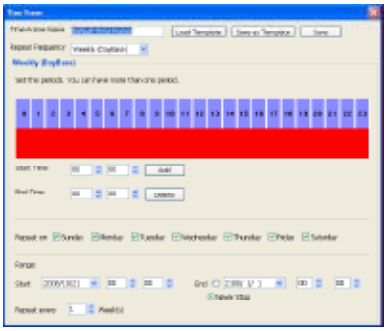


Figure 7.6 On-schedule recording

In an IP surveillance system, the frame rate is changeable. Therefore, users can set the system to use a lower frame rate during live monitoring for low bandwidth usage while shifting to a full frame rate during event-triggered recording to ensure good image quality (Figure 7.7).

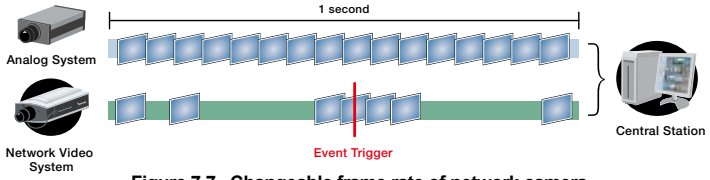


Figure 7.7 Changeable frame rate of network camera

7.2.3 Playback

Recorded video images can be viewed in multiple split windows and by several users at the same time. The recorded database can also be searched in a more efficient way such as by date, time, region or event.

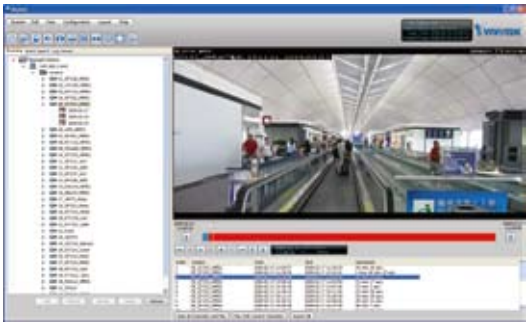


Figure 7.8 Video playback

7.2.4 Management

Through the management interface of the software, users can make various configurations of video images, set up and manage various parameters, such as recording schedule and event trigger conditions.

7.3 Advanced Features

7.3.1 E-map

The E-map functionality gives users an overview of the system and helps them quickly locate each camera. When an incident occurs, the related camera will be marked and the user can immediately switch to the images of that camera (Figure 7.9).

Figure 7.9 E-map improves camera management efficiency

7.3.2 Auto-backup

Auto-backup enables users to back up data regularly and automatically, providing a more reliable IP surveillance system.

7.3.3 Failure Report

Failure reports that display a history of system errors can help users solve problems more efficiently.

7.4 Digital I/O Devices

Digital input and output ports connect network cameras to external security devices such as alarms and sensors, strengthening the surveillance system's detection and alerting capability.

7.4.1 Digital Input Devices

- **Glass break sensor:** the device can detect specific frequency of sounds and vibration, for example, glass breaking. It is usually installed by the window to detect glass window breaking caused by burglary.
- **Active infrared sensor:** the device emits infrared light to detect intruding objects. When the infrared beam is blocked, alerting signals will be sent. It is usually used for outdoor applications.
- **Smoke sensor:** the device can detect dust concentration in the air. Mainly used for fire detection, the sensor sends out alerting signals when the concentration of the dusts exceeds a given value.
- **PIR (passive infrared sensor):** the device can detect object movement by the infrared light emitted from the object caused by its temperature.It is ideal for indoor use.

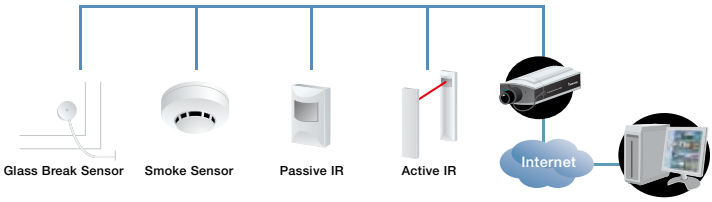


Figure 7.10 Connection of digital input devices

7.4.2 Digital Output Devices

- **Alarm:** when incidents occur, alarms will send out high frequency of sounds to notify security staff or visitors.
- **Alert light:** alert lights inform the security staff of an incident with flashlight, such as xenon flashlight.
- **Remote transmitting system:** warning signals are to the control console to prompt more comprehensive reaction.

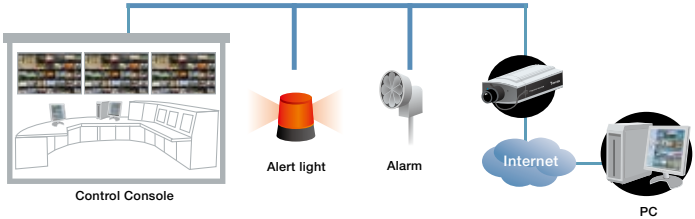


Figure 7.11 Connection of digital output devices

7.5 Manage Large Systems

For a large surveillance system that consists of dozens or hundreds of network cameras, server/client-based central management software is needed so as to provide flexible and scalable management. By installing server/client software in separate PCs, users can manage cameras remotely in any places.

VIVOTEK's central management software ST7501 features reliable recording, easy system management, and great scalability for diverse IP surveillance applications. With server/client structure, users can carry out remote management on a large-scale system and benefits from a robust IP surveillance system.

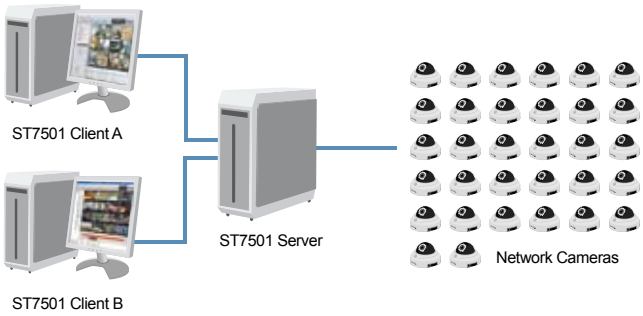


Figure 7.12 VIVOTEK ST7501 central management software

Chap.8
Applications

Network cameras are being used in a variety of industries, from professional to personal applications. As each industry has different demand for surveillance, their requirements for network camera types and functions vary. This chapter presents major network camera applications along with useful tips for selecting the right kind of cameras.

IP surveillance applications can be mainly categorized as professional, SMB (Small- and Medium-sized Business), 3GPP and home applications. Professional applications require more advanced features to cope with the high demands they face. For SMB applications, surveillance systems featuring basic monitoring and management functions can meet most of the needs. In home applications, IP surveillance systems are used not only for home security but also for keeping track of the activities in the home when parents are away from home. 3GPP applications allow for real-time monitoring and control on the move. With a 3G phone, anyone can be kept updated with the latest traffic information, status in the office or activities in the home.

Apart from security, new applications are emerging. For example, the National Taiwan University integrated a VIVOTEK PT7135 in a robot to have it served as a guide dog for the blind. Such robots can also carry out investigation in dangerous areas to avoid possible harm to human lives. Entertainment is another application with increasing importance. As an example, VIVOTEK FD7131 and IP6122 were used to monitor racing pigeon movement during contests held in Zhejiang, China. For more information, please go to Success Stories page under the Product section on VIVOTEK website.

The following table lists the main placement of network cameras and provides some recommended features for each application.

Camera Placement	Recommended Features
Large outdoor places (airports, parking lots, parks, etc.)	Day and night, vandal-proof, IP66-rated, pan/tilt/zoom, megapixel, intelligent, weather-proof
Small outdoor places (building perimeter, alleys, etc.)	Day and night, vandal-proof, weather-proof, IP66-rated
Large indoor places (stations, halls, stadiums, etc.)	Vandal-proof, pan/tilt/zoom, megapixel, intelligent
Small indoor places (room, corridors, stairway, elevators, etc.)	PoE
Control rooms	Two-way audio
Places with moving objects (highways, train/bus stations, etc.)	Progressive scan CCD, intelligent
High contrast places (ATMs, parking lot entrances, etc.)	WDR

Chap.9
System Design

9.1 Identifying Customers Needs

Before deploying an IP surveillance system, having a layout map of the site at hand to identify the shooting purposes of each network camera is necessary and useful. The map gives you an overview of the installation site and helps you have an in-depth discussion with your customers. You can have a more general idea about the number of cameras the whole system needs, cabling scheme, and other peripherals such as speakers, microphones, and joysticks required so as to achieve an efficient installation.

Generally, cameras are used for viewing or recording, or both of them. For special requirements such as object tracking, people counting, motion detection or plate identification, intelligent capability in cameras or software will be needed.

9.1.1 Viewing Considerations

The following factors should be your main considerations when installing a network camera.

Viewing Direction

The shooting direction determines the lens and camera types, placement, or even the coverage of a camera. Bear in mind that cameras' shooting direction should be in line with the direction of illumination to minimize the influence of backlighting on image quality. Sometimes people may feel uneasy with the cameras pointing at them; in this case, you may choose cameras with a smoke cover.

Viewing Distance

A camera with zoom capability is needed if you want to capture close-up images of an object at a distant. The zoom time will determine how close you need. A vari-focal lens offers a small zoom capability, which is adjusted manually via a controller.

Viewing Angle

If the monitored area is a wide open field, a camera with PTZ movement or a wide angle lens is highly recommended. PTZ cameras can instantly move to a position you want to see by a click on browser or software. A wide angle lens may offer extensive coverage of depth-of-view, but suffer barrel distortion.

Viewing Object

In case of monitoring a fast moving object such as vehicles, it is highly suggested to use a camera with a progressive scan CCD sensor. Progressive technology can help you generate clear-cut images without jagged edges; but the interlaced technology happens.

9.1.2 Environmental Considerations

CCTV Cameras

Since customers tend to expect to keep the existing analogue CCTV cameras for the sake of lowering investments, you may adopt a video server to help them easily migrate to IP surveillance.

Outdoor/Indoor

Outdoor applications for network cameras usually require the features of vandal- and weather-proof, and conformation to the IP66-rated standard for protection against vandalism or weather damage. Furthermore, to cope with very harsh temperature environments, a fan and heater is a must. In addition, the cameras should have an auto-iris lens to protect them from damage caused by strong sunlight.

Light

The quality of the captured image is significantly influenced by light sources in the monitored area. For most of the conditions you encounter, VIVOTEK provides different products to meet your specific needs as follows.

Day and Night

For outdoor applications where light changes significantly during daytime and nighttime, the true day and night function (camera with a removable IR-cut filter together with IR illuminators) is required so as to maintain good image quality constantly for 24 hours.

Low Light

A camera with better light sensitivity (low light performance) indicates that it can generate acceptable image quality in low-lux environments. VIVOTEK's full-range cameras provide fairly good low light performance.

Challenging Light

For such high contrast places as entrances, ATMs and loading areas, cameras with WDR can still cope with the challenging light to generate identifiable image with ease.

Mounting

After deciding the shooting direction and the height for camera placement, you must find a suitable mounting kit for places such as walls, ceilings, poles, roofs or corners to have your camera installed. VIVOTEK provides a variety of mounting kits to facilitate your installation.

Power Outlet

You should check if there are power outlets nearby the locations of the cameras for easy access. If it is a concern, a network camera featuring PoE or the addition of a set of PoE kit will easily help you solve this problem that analogue camera cannot.

Wireless/Wired Connection

Wireless connection is often applied in a wide open space or where the decor requires high protection or no Ethernet outlets provided. Without the cabling, you can greatly decrease the cost and get rid of the problem of tangled cabling. Most of buildings now have Ethernet outlets as infrastructure, with which you can significantly reduce the workload of cabling but the CCTV security must pay for.

Audio

When installing audio-enabled cameras, audio cables must be kept away from power cables and high-frequency signal cables so as to reduce interference. In addition, microphones should be placed near the sound source and away from speakers.

Bandwidth

The bandwidth capacity is another key point during video transmitting. Regarding the calculation formula of bandwidth, please refer to the Chapter 6. If upgrade is needed, please consult with your local ISP.

Storage

There are many factors affecting storage requirements. For more information, please refer to Chapter 6.

Decor

Wireless or PoE technologies can greatly help you deal with the decor concerns caused by the tangled cabling. Additionally, dome type allows cables to be hidden so as to better fit in with the decor of the building.

DI/DO

If you customers need to connect external deices for different application, network cameras with digital input/ output ports are required. Digital input ports connect with sensors such as infrared motion detectors or glass break sensors while digital output ports connects with alarms.

Operational Requirement Checklist

A checklist will help you plan an IP surveillance that truly addresses your customer's needs (Table 9.1).

Table 9.1 Pre-installation checklist

Section 1: Purpose

- What is the purpose of surveillance?

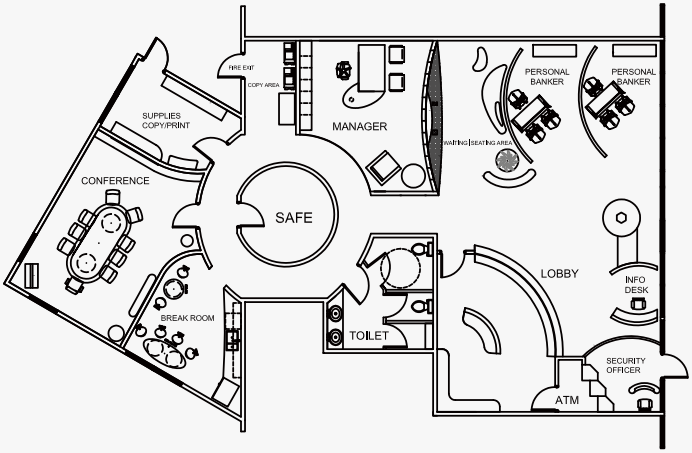
☐ Monitoring ☐ Viewing ☐ Recording ☐ Tracking ☐ Counting

☐ Crime Deterrence / Prevention Of Crime

☐ Detection ☐ Recognizing ☐ Identifying

☐ Others_____

Section 2: Floor plan of the monitored site



Section 3: Location

- Where is the camera sited? (camera location)
  ☐ Large outdoor places ☐ Small outdoor places ☐ Large indoor places
  ☐ Small indoor places ☐ Control rooms ☐ Places with moving objects
  ☐ High-contrast environments ☐ Others _____
- Number of cameras to be installed?
- Types of camera to be installed?
  ☐ Fixed ☐ PTZ ☐ Fixed Dome ☐ Speed Dome
- Targets to be observed? (who/what/where)
- Does it monitor any other area not intended? (e.g., private gardens)
  ☐ Yes ☐ No

Section 4: Environmental considerations

- Outdoor/Indoor
  ☐ Outdoors ☐ Indoors ☐ Vandal-proof housing
  ☐ Weather-proof housing ☐ Fan ☐ Heater
- Lighting conditions
  ☐ Natural ☐ Artificial ☐ Day/Night ☐ Low light ☐ Challenging light
  ☐ Infrared illuminators required ☐ White-light lamps required
  ☐ Auto-iris required
- Installation position
  ☐ Wall ☐ Ceiling ☐ Pole ☐ Roof ☐ Corner ☐ 3-axis required
  ☐ Others _____
- Power and connection
  ☐ PoE required ☐ Wireless required ☐ Power supply ☐ UPS
- Audio
  ☐ 2-way audio required
- Bandwidth
  _____Mbps

Section 5: Image quality

- Image resolution required
  ☐ VGA ☐ 1.3M ☐ 2M
- Frame rate appropriate to the target's speed
- Compression techniques for recording

Section 6: Alert functions

- What response is needed for an event or activity?
  ☐ Trigger audible alarm ☐ Trigger visual alarm
  ☐ Send text message or images ☐ Emergency relay to police

Section 7: Viewing Terminals

☐ 3G phones ☐ PCs ☐ TVs

Section 8: Recording

- How long will data be reserved?
- How many cameras' images to be recorded simultaneously?
- Any additional information to be recorded with the image?
- Compression techniques for recording?

Section 9: Maintenance

- Equipment should be in good working order, well maintained and serviced on a regular basis
- Cameras should be protected from any physical/environmental risks (e.g., vandalism)

9.2 System Planning

Based on the survey above, you can get started with a comprehensive system design plan and select appropriate cameras, back-end hardware and software for your customers now.

9.2.1 Camera Considerations

Indoor or outdoor application is the first concern when selecting a camera. Other important camera features such as day and night, resolution (Megapixel or VGA), cabling (PoE or wireless) and compression formats (MJPEG, MPEG-4 or H.264) or other alternatives will also be main considerations for identifying an exact network camera.

9.2.2 Hardware Considerations

Computer
PC hardware requirements must be higher than 1.7GHz processor and 256MB memory. Free-bundled software has to be run on Microsoft Windows 2000/XP/Vista.

PoE Switch/Wireless Access Point
PoE switches must be deployed if you are installing PoE-enabled cameras. For wireless connection, you need to prepare a wireless access point.

NVR
You can have an NVR as a dedicated storage device so as to prevent surveillance video data from sharing the storage space of PCs.

9.2.3 Software Considerations

Internet Browser
Internet Explorer 6.0 or above and Mozilla Firefox must be installed so as to view video images on PCs. For cellular phone, 3GPP player is required.

Central Management Software
For a video surveillance system, viewing, recording, playing back, and managing videos are basic functionalities. VIVOTEK offers reliable free-bundled 32-CH ST7501 central management software to meet your various requirements.

Other Software
Besides central management software, many customers expect to have more advanced functions such as intelligent analytics for a variety of applications. VIVOTEK has been working closely with numbers of well-known software partners as our SIA (Software Integration Alliance). For any specific need, you may check out our website at http://www.vivotek.com/alliance/siaprogram.html for further information.

9.3 Installation and Check

9.3.1 On-site Installation

Based on the abovementioned plan, you can start to install the surveillance system.

9.3.2 Post-installation Checks

One the installation is over, it is necessary to perform post-installation checks. Below is a checklist that helps you ensure a successful installation.

Table 9.2 Post-installation checklist

Section 1: Image quality
☐ Can each camera provide coverage as planned?
☐ Can images be rendered clearly?
☐ Can each camera provide sufficient frame rate?
Section 2: Alert functions
☐ Can alarm sensors be triggered as expected?
☐ Can security staff and administrators be alerted immediately?
Section 3: Viewing Terminals
☐ Can video be displayed appropriately on viewing terminals?
Section 4: Recording
☐ Can recorded data be located correctly?
☐ Can images be well preserved before being overwritten?
Section 5: Export/Archiving
☐ Can export and archiving functions work normally?

9.4 Operational Training

Security staff, system operators and managers must be trained to know how to operate the system and what they should do when an incident occurs.

Table 9.3 lists necessary training items for security staff/operators and managers.

Table 9.3 Operational training requirements

Security guards/operators		Administrators
Hardware	Software	
Configuration	Configuration	Remote monitoring
Troubleshooting	Troubleshooting	Remote playback
Authorization	Authorization	Passwords
Remote monitoring	Remote monitoring	Image search
Image quality configuration	Image quality configuration	
Functional configuration	Functional configuration	
	Back-up	
	Response to alarms	
	Recording configuration	

9.5 System Maintenance

Regular maintenance is required in order to ensure optimal performance and longer lifespan for the system. Short-term maintenance must be performed regularly, for example, twice a year. For long-term maintenance, it is important to select a vendor that provides a long-term warranty so as to ensure every component is available when replacement is needed. VIVOTEK provides a warranty of one to three years, depending on different products. With 130 distributors worldwide, VIVOTEK can provide comprehensive maintenance services.

During maintenance, all equipment must be inspected thoroughly. Make sure all components as well as connections and cabling are in good conditions without rustiness, erosion or damage. It is also important to confirm with the clients or examine the system during maintenance to see if the system needs expansion.

Chap.10
Intelligent Video Systems

10.1 Introduction

The need to retrieve useful data in a more efficient way and to provide more prompt response has contributed to the development of intelligent video systems. The architecture of an intelligent video system mainly includes the centralized and distributed types.

10.2 Architecture

10.2.1 Centralized Platform

A centralized intelligent video system performs video content analysis at the back-end. It uses an intelligent DVR featuring high computing capabilities to analyze and process data from all cameras.

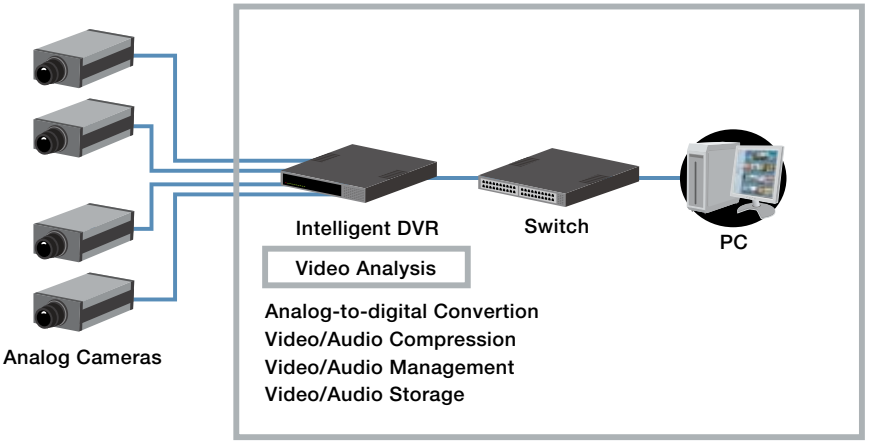


Figure 10.1 Video content analysis in centralized architecture

10.2.2 Distributed Platform

A distributed intelligent video system uses intelligent network cameras to analyze video content in real time so as to enable prompt response. The architecture can be easily expanded by adding new cameras.

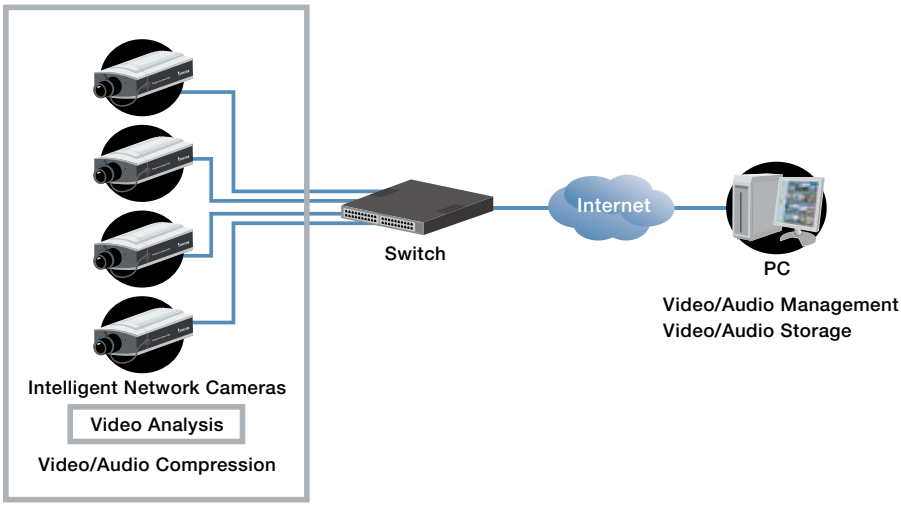


Figure 10.2 Video content analysis in distributed structure

Compared with centralized architecture, a distributed intelligent video system provides benefits in deployment costs, bandwidth requirements and content accuracy (Table 10.1).

Table 10.1 Comparison of centralized and distributed intelligent video systems

Platform	Centralized	Distributed
Features	■ High CPU requirements ■ Lower recording search efficiency	■ High performance with minimum investment ■ Higher accuracy from pre-compression image processing ■ Higher bandwidth efficiency

10.3 Advantages of Distributed Architecture

Since a distributed intelligent video system has video content analyzed by the front-end cameras, it offers the following benefits.

Real-time Analysis and Response
Because captured images are analyzed in real time at the camera side, unusual activities can be detected immediately. This allows for prompt response such as notifying security staff.

Reduced Labor Costs
An intelligent video system can constantly concentrated on analyzing and processing data, significantly reducing the number of security staff and the travel costs resulting from on-site maintenance.

Decrease in Server Workload, Storage Space and Bandwidth Usage
Because only event relevant and needed information is transmitted to the back-end system, server workload is significantly reduced. It also cuts down bandwidth usage and storage requirements.

Scalability and Integration
Intelligent video systems can be integrated with other systems to serve purposes beyond security, such as in combination with access control system for more efficient entrance management or with retail POS systems to provide customer information. Further, during expansion, users can simply add new intelligent cameras at the front end without needing to upgrade the back-end system for stronger processing capability.

10.4 Detection

10.4.1 Tamper Detection

Tamper detection can detect and respond when the camera is redirected, defocused, blocked or spray-printed. It allows cameras to be installed in tampering-prone places such as transportation stations or prisons.

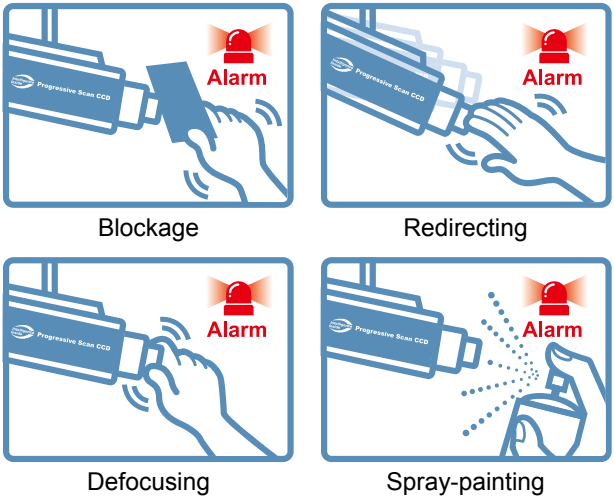
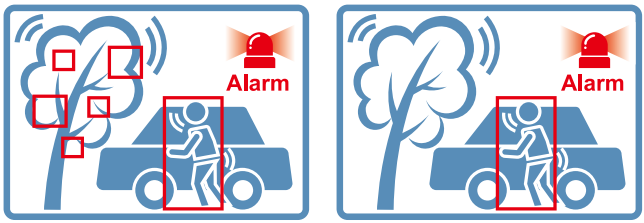


Figure 10.3 Tamper detection

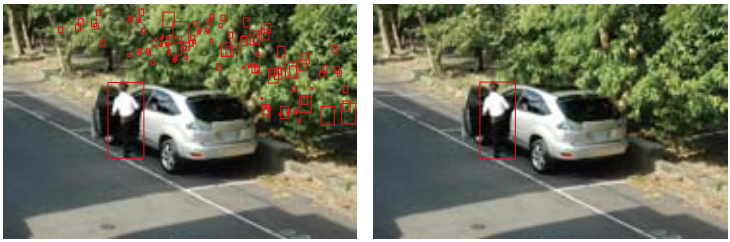
Figure 10.4 Alarm triggered by tamper detection

10.4.2 Intelligent Motion Detection

Intelligent motion detection can distinguish moving objects of interest motions from natural movements and trigger alarms based simply on object motions. The function, mainly for outdoor applications, can eliminate false alarm rates due to environmental noise that appears with conventional motion detection.



Conventional Motion Detection Intelligent Motion Detection

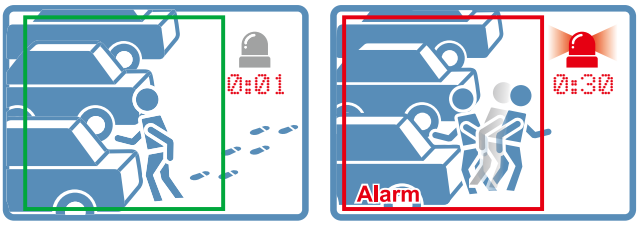


Conventional Motion Detection Intelligent Motion Detection

Figure 10.5 Comparison of conventional and intelligent motion detection

10.4.3 Loitering Detection

Loitering detection can detect an object or a person that has been staying in a predefined area over a period of time. The function effectively prevents crimes because suspicious objects or activities are detected before damage is caused.



Presence of Lingering Object Alarm Triggered after 30 Seconds

Figure 10.6 Alarm triggered by loitering detection

10.4.4 License Plate Recognition

License plate recognition can identify the plate number of a vehicle and match the information with the data in the police database. Besides tracking down criminals, license plate analysis can also be used for traffic control and parking lot management.

Figure 10.7 License plate recognition

10.4.5 People Counting

People counting can calculate the amount of people in an area and provide the information for business management, such as the number of customers entering the shop or the number of customers waiting in a line.

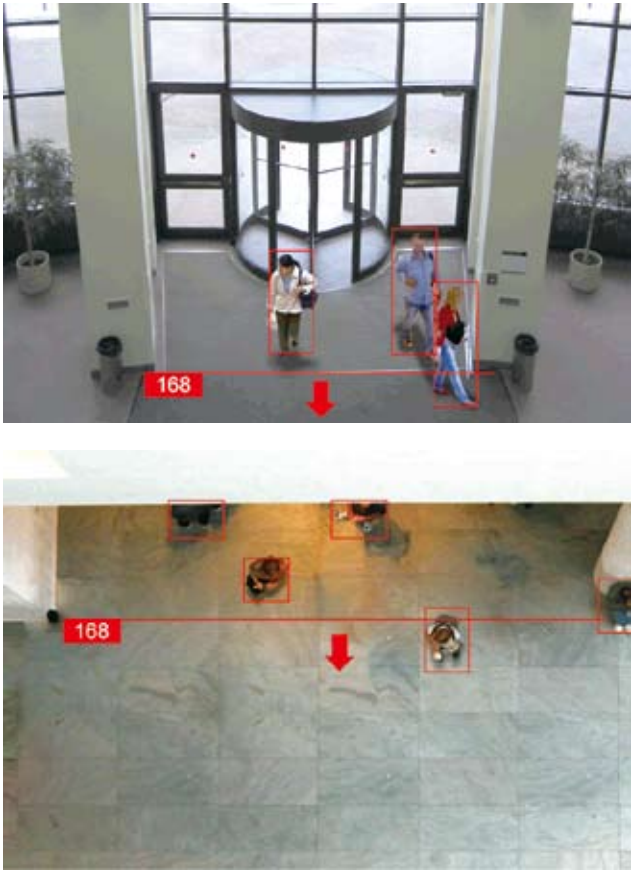


Figure 10.8 People counting

Glossary

A

AE
Auto Exposure, a system for automatically setting the proper exposure according to the existing light conditions. There are three types of AE systems: programmed, aperture-priority, shutter-priority

AES
Automatic Electronic Shutter, the sensor will automatically adjust the sensitivity according to the changes in illumination of detected area.

AF
Auto Focus, an ability by which the camera lens automatically adjusts its focus on the captured subject.

AGC
Automatic Gain Control, an electronic circuit which amplifies the video signal when the signal strength falls below a given value due to the lack the light on the image device.

Auto-iris
A special type of iris, is used to adjust the amount of enter light, electrically controlled by the camera. There are two main types of auto-iris: Video-drive and DC-drive iris. See also Video-drive Iris and DC-drive Iris.

AWB
Automatic White Balance, is used in digital camera to automatically compensate the type of light (daylight, fluorescent, incandescent, etc.,) or lighting conditions in the scene. To make it normal for the human eye.

B

Bit Rate
A unit of speed, defines the number of bits/time unit, usually expressed in Kbit/s or Mbit/s.

C

CE
Consultants Europe, is a Technical and Legal organization specialized in the CE marking, CE certification and Authorized Representation of products.

Codec
Codec stands for Coder/ Decoder, which converts analog video and audio signals into a digital format for transmission. The codec also converts received digital signals back into analog format.

Contrast
Contrast is usually defined as a ration between the darkest and the brightest posts of an image in image processing Images have a higher contrast level generally display a greater degree of color grayscale variation than those of lower contrast.

D

DC-drive Iris
One type of auto-iris, will automatically adjust the amount of light allowed to enter. It requires simply a DC input from the camera without signal converted.

Digital Zoom
Digital zoom takes part of the image and expends it. The resulting image appears bigger but not as sharp as with an optical zoom.

D-SUB
D-SUB is used to indicate the type of connector for the VGA interface.

F

FCC
Federal Communications Commission, is responsible for a administering the television and radio airwaves, satellite and cable transmissions, and telegraph communications.

Fixed Iris
Fixed iris lens is one kind of iris and with fixed size iris.

Frame Rate
The rate at which video frames are displayed on a monitor per second. Frame rate for PAL is 25 fps, and frame rate for NTSC is 30 fps.

H

Hue
It is an attribute of color and the other two elements are brightness and saturation. Hue differences depend primarily on the variations of wavelength and defined by its dominant wavelength.

I

IGMP
Internet Group Management Protocol, is a protocol that manages PCs' multicast group membership. It provides the membership information of a PC to a multicast router, which sends out queries periodically to confirm the status of that PC. A PC can request to join in a specific group, and when it becomes a member of that group, it will receive data designated to that group.

M

MAC Address
Media Access Control address, is one unique code assigned to a networking device. For example, the network card in a computer has its own MAC address.

O

Optical Zoom
Optical zoom amplify the image size by adjusting the lens. It enlarges the subject without sacrificing resolution.

P

Proxy Server
A server that provides the service for clients to make indirect network connections to other network services.
Proxy server will save the previous data or resource in a cache when the request is made for first. To provide it when the same request is made again. It could be used to avoid occupying much bandwidth.

R

RS-485
RS-485 is an electrical specification of a two-wire, half-duplex, multipoint serial connection. It supports high data transmission speeds and uses a different balanced line over twisted pair. It also spans large distances.

RTCP
Real-Time Control Protocol, is used to monitor the session. It is mainly used to feed the streaming server with reception statistics from the client. The server may then decide to use these statistics (such as the numbers of lost packets, the delay from reception) to adapt its strategy.

RTP
Real-Time Transport Protocol, is the protocol used to transport the multimedia stream to the client. It sends a packet to the network but cannot warrant that the packet will reach its destination.

S

Saturation
A measurement of chrominance, or the intensity of color in the video signal.

V

Video-drive Iris
One type of auto-iris, a Video-drive iris lens has an amplified circuit for converting input video signal to a DC input for the camera.

Notes

All specifications are subject to change without notice.
Copyright © 2009 VIVOTEK INC. All rights reserved.
P/N:0120001O5

VIVOTEK
BUILT WITH RELIABILITY

use-IP

www.use-ip.co.uk
01304 827609

VIVOTEK INC.
6F, No.192, Lien-Cheng Rd., Chung-Ho, Taipei County, Taiwan
Tel: +886 2 8245 5282 Fax: +886 2 8245 5532
E-mail: sales@vivotek.com http://www.vivotek.com

VIVOTEK USA INC.
470 Lakeside Drive Suite C, Sunnyvale CA 94085
Tel: 408-773-8686 Fax: 408-773-8298
E-mail: salesusa@vivotek.com